Technical Report 910

Deceiving the Opposing Force: A Program of Theoretical and Applied Research to Aid the Deception Planner

Allen L. Zaklad
Analytics, Inc.

Wayne W. Zachary and James H. Hicinbothom
CHI Systems, Inc.

Alfons L. Broz
Analytics, Inc.

Beverly G. Knapp
U.S. Army Research Institute

September 1990

United States Army Research Institute
for the Behavioral and Social Sciences

U.S. ARMY RESEARCH INSTITUTE FOR THE BEHAVIORAL AND SOCIAL SCIENCES

A Field Operating Agency Under the Jurisdiction of the Deputy Chief of Staff for Personnel

EDGAR M. JOHNSON **Technical Director**	**JON W. BLADES** **COL, IN** **Commanding**

Research accomplished under contract for the Department of the Army

Analytics, Inc.

Technical review by

David D. Burnstein
James Fox

NOTICES

DISTRIBUTION: Primary distribution of this report has been made by ARI. Please address correspondence concerning distribution of reports to: U.S. Army Research Institute for the Behavioral and Social Sciences, ATTN: PERI-POX, 5001 Eisenhower Ave., Alexandria, Virginia 22333-5600.

FINAL DISPOSITION: This report may be destroyed when it is no longer needed. Please do not return it to the U.S. Army Research Institute for the Behavioral and Social Sciences.

NOTE: The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION
Unclassified

1b. RESTRICTIVE MARKINGS
--

2a. SECURITY CLASSIFICATION AUTHORITY
--

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE
--

3. DISTRIBUTION/AVAILABILITY OF REPORT
Approved for public release;
distribution is unlimited.

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
--

5. MONITORING ORGANIZATION REPORT NUMBER(S)
ARI Technical Report 910

6a. NAME OF PERFORMING ORGANIZATION
Analytics Incorporated

6b. OFFICE SYMBOL (If applicable)
--

7a. NAME OF MONITORING ORGANIZATION
U.S. Army Research Institute
Field Unit at Fort Huachuca

6c. ADDRESS (City, State, and ZIP Code)
2500 Maryland Road
Willow Grove, PA 19090

7b. ADDRESS (City, State, and ZIP Code)
ATTN: PERI-SA
Fort Huachuca, AZ 85613-7000

8a. NAME OF FUNDING/SPONSORING ORGANIZATION U.S. Army Research Institute for the Behavioral and Social Sciences

8b. OFFICE SYMBOL (If applicable)
PERI-S

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
MDA903-86-C-0403

8c. ADDRESS (City, State, and ZIP Code)
5001 Eisenhower Avenue
Alexandria, VA 22333-5600

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.
62785A	790	1306	C03

11. TITLE (Include Security Classification)
Deceiving the Opposing Force: A Program of Theoretical and Applied Research to Aid the Deception Planner

12. PERSONAL AUTHOR(S) Zaklad, Allen L. (Analytics, Inc.); Zachary, Wayne W., Hicinbothom, James H. (CHI Systems, Inc.); Broz, Alfons L. (Analytics, Inc.); and Knapp, (Continued)

13a. TYPE OF REPORT
Final

13b. TIME COVERED
FROM 88/10 TO 89/12

14. DATE OF REPORT (Year, Month, Day)
1990, September

15. PAGE COUNT

16. SUPPLEMENTARY NOTATION
Dr. Beverly G. Knapp, Contracting Officer's Representative

17. COSATI CODES

FIELD	GROUP	SUB GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)

Deception	Deception planning
Military deception	Battlefield deception
Tactical deception	Deception vulnerability (Continued)

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The concept of battlefield deception was developed using a hierarchical framework, a cognitively based decision model, and an act-react cycle to illustrate battlefield flow to help deception planners understand intentions and expected observables. Based on identified gaps in the current doctrinal planning process, a PC-based battlefield activities analysis tool (BAAT) was designed. The explication of the planning process, U.S. and Soviet decision cycles, and the BAAT system provide a set of products and tools to enhance U.S. Army deception planning and doctrine development. Key words. Battlefield, Deception; military doctrine; [illegible] (RWJ)

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL
Beverly G. Knapp

22b. TELEPHONE (Include Area Code)
(602) 538-4704

22c. OFFICE SYMBOL
PERI-SA

Previous editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

ARI Technical Report 910

12. PERSONAL AUTHOR(S) (Continued)

Beverly G. (ARI Field Unit at Fort Huachuca)

18. SUBJECT TERMS (Continued)

OPFOR deception cycle
Pathfinding

Technical Report 910

Deceiving the Opposing Force: A Program of Theoretical and Applied Research to Aid the Deception Planner

Allen L. Zaklad
Analytics, Inc.

Wayne W. Zachary and James H. Hicinbothom
CHI Systems, Inc.

Alfons L. Broz
Analytics, Inc.

Beverly G. Knapp
U.S. Army Research Institute

Field Unit at Fort Huachuca, Arizona
Julie A. Hopson, Chief

Systems Research Laboratory
Robin L. Keesee, Director

U.S. Army Research Institute for the Behavioral and Social Sciences
5001 Eisenhower Avenue, Alexandria, Virginia 22333-5600

Office, Deputy Chief of Staff for Personnel
Department of the Army

September 1990

Army Project Number
2Q162785A790

Human Performance Effectiveness and Simulation

Approved for public release; distribution is unlimited.

FOREWORD

The Fort Huachuca Field Unit of the U.S. Army Research Institute for the Behavioral and Social Sciences (ARI) performs research in support of key areas of interest to the U.S. Army Intelligence Center and School (USAICS) and the greater military intelligence (MI) community. In the research reported here, ARI brings to bear the results of cognitive and organization analysis to assist the proponents of battlefield deception.

Deception can serve as a powerful force multiplier and is one member of the family of C3CM (Command, Control, Communications Countermeasures) that also includes electronic warfare (EW) and operations security (OPSEC). Deception planning is primarily the responsibility of operations planners, yet support for the planning is dependent on considerable interaction with intelligence personnel. This report contributes to the scientific understanding of battlefield deception by analyzing the OPFOR (Opposing Force) decision-making process, providing approaches to manipulating this process via deception, and describing a battlefield activities analysis tool (BAAT) that was developed to assist the deception planning and analysis process.

Other work in this research program are in the form of ARI reports, including a framework for battlefield deception, deception planning methods, and an overview of OPFOR and U.S. planning processes for deception. Results of this research program have been briefed to the CG, USAICS; the DOD Camouflage, Cover, and Deception Technical Review Group; and the U.S. Air Force Special Operations School.

EDGAR M. JOHNSON
Technical Director

ACKNOWLEDGMENTS

This project has benefited greatly from support and guidance from Drs. Beverly Knapp and Julie Hopson at the U.S. Army Research Institute for the Behavioral and Social Sciences (ARI) Field Unit at Fort Huachuca, Arizona, and from the Battlefield Deception Office, U.S. Army Intelligence Center and School (USAICS), Fort Huachuca, Arizona.

Thanks to Phyllis Martin for her skillful editing and competence and enthusiasm in managing the production of this report. Dan Scolaro, William Driver, and Lorna Ross helped to design and implement the deception planning aids. We thank Heidi Langdon for her able handling of the diverse administrative tasks.

The views, opinions, and/or findings contained in this report are those of the authors and should not be construed as an official Department of the Army position, policy, or decision.

DECEIVING THE OPPOSING FORCE: A PROGRAM OF THEORETICAL AND APPLIED RESEARCH TO AID THE DECEPTION PLANNER

EXECUTIVE SUMMARY

Requirement:

To support the more effective utilization of battlefield deception by Army and other service personnel by developing cognitively based approaches, tools, and aids for the deception planner, trainer, and developer of doctrine.

Procedure:

The concept of battlefield deception was developed using a framework and analytical techniques to elaborate the planning process, providing a hierarchical language with which to talk about deception. Relevant decision processes were defined and systematized into an act-react model containing the concepts of reinforcement, intentions and observables, and pathfinding. In addition, a PC-based aid, called the battlefield activities analysis tool (BAAT) was designed. The BAAT assists the planner by providing databases on intentions and observables in various offense and defense scenarios, which can be used as part of a wargaming process to develop deception plans.

Findings:

Five key problem areas for deception planners were defined from the conceptual framework: (1) determining how the United States wants the OPFOR (Opposing Force) to act; (2) understanding what perceived situation would cause the desired action; (3) determining what battlefield information would cause the desired OPFOR perception; (4) understanding how to manipulate the battlefield information; and (5) determining how to use available resources to portray the desired perception. From these problem areas, it was determined that the soldier requires more assistance in the "how to" process (problem areas 1-3) of deception planning than in the execution of formulated plans. The determination of U.S. and OPFOR intentions using a cognitive wargaming model and principles of behavioral reinforcement provided the optimal basis for planning to occur. Understanding the perceived situation on both sides and determining what impact various information signatures would have were determined as critical. The prototype BAAT system was seen as an important component in assisting the overall planning process, since the databases and their manipulation allow planners to "see" outcome consequences.

Utilization of Findings:

The products of this research will provide practical benefits by giving a systematic understanding of deception as the manipulation of intentions and activities in an act-react cognitive wargaming model. In the near term, the results and BAAT system provide a foundation for enhanced deception planning to build on current doctrine. In the longer term, the evolution of the act-react cycle analysis and enhanced BAAT system will lead to an operational planning system that will extend beyond deception into other operation planning areas.

DECEIVING THE OPFOR: A PROGRAM OF THEORETICAL AND APPLIED RESEARCH TO AID THE DECEPTION PLANNER

CONTENTS

LIST OF FIGURES

1. INTRODUCTION

Background and Purpose

Military deception is a highly specialized, discreet, and sophisticated art of warfare. Throughout history, it has successfully supported and enhanced victorious efforts on the battlefield. In recent years, battlefield deception has gained increasing attention as a potential "force multiplier" and an effective way of "fighting smarter." The charter for battlefield deception stems directly from the AirLand Battle Doctrine. In the past decade, Defense Science Board studies, which in part led to today's AirLand Battle Doctrine, have recommended that battlefield deception be a systematic, integral part of overall decision making and planning. These studies also recommended that it should be consistent with both: (1) command, control and communications countermeasures (C3CM) operations, and (2) operations plans that incorporate deception at echelons above corps (EAC).

Deception is one member of the family of C3CM activities that also includes electronic warfare (EW) and operations security (OPSEC). EW focuses on attacking the enemy's command and control systems, primarily through affecting electronic communications systems and electronic intelligence-gathering devices. OPSEC focuses on denying information, where possible, and controlling information about friendly capabilities and intentions that might be of value to the enemy. Deception planning is primarily the responsibility of the operational planners in the G3 section's deception cell. However, support for their planning requires considerable interaction with the G2 section (intelligence). Deception functions properly only if the staff elements involved fully coordinate their efforts toward support of their commander's decision making.

Battlefield deception is the process of misrepresenting the battlefield situation or friendly force (FFOR) capabilities and intentions. The purpose of this misrepresentation is to induce the opposing force (OPFOR) into behaving in a way more desirable to the FFOR than would be likely without the deception. A major assumption of the effort reported in this document is that battlefield deception planning may be viewed as being based on solving five key problems:

(1) Determining how the FFOR wants the OPFOR to act;

(2) Understanding what perceived situation would cause the OPFOR commander to act in the specified desirable way;

(3) Determining what information and intelligence, from what sources, would get the OPFOR commander to perceive the battlefield situation in the desired way;

(4) Understanding how to manipulate the intelligence data collected by the OPFOR to cause the OPFOR commander to get the desired information and intelligence from the necessary sources; and,

(5) Det. rmining how to use the resources available to the FFOR to manipulate that data as desired.

A critical issue in deception is that current military views of conducting deception focus primarily on the fourth and fifth problems, leaving the first three virtually untouched.

A second important issue in the Army's current approach to deception planning is the lack of adequate planning doctrine. A major step toward resolving this lack was the codification of US Army doctrine in Field Manual 90-2, "Battlefield Deception" (US Army, 1987). This doctrine is a necessary beginning, but is limited in its scope: **FM 90-2 outlines "what" needs to be done, but does not explain "how."** The "how" requires understanding the OPFOR decision cycle and its vulnerabilities, and then exploiting these vulnerabilities through the deception planning process. Deception knowledge or deception "science" is vague and poorly defined despite the new Army doctrine.

This report summarizes the results of a three-year effort by the Army Research Institute to address these two issues via psychological analyses of military decision making. In particular, it was seen that if one takes seriously that deception must be based on the above five problems, then two things become clear. First, adequate doctrine must be based on addressing all the five problems. Second, the first three, i.e., those that are **not** part of publicly acknowledged deception doctrine and training, are clearly in the realm of decision making and cognitive performance. Therefore, this project was intended to address those first three problems through study of the relevant decision making processes, and thereby systematize understanding of deception. The eventual end goal of the project was to aid the battlefield deception planner in the systematic accomplishment of the deception task.

2. A TAXONOMY OF THE COMPONENTS OF DECEPTION

Introduction: A Framework for Tactical Deception

A *framework* is a set of interrelated structures, categories, and/or models that define a domain. A *domain*, e.g. tactical deception, is a set of individual problems or problem instances that may be similarly treated because they share common features that allow them be solved in a common manner. A framework defines this underlying similarity and structure as explicitly and precisely as possible. A deception framework is directed at the interdependencies within the domain of tactical deception for purposes of helping to understand and solve problems of tactical deception.

There are least four kinds of integrating functions that can be guided by the deception framework. The first and main use of the framework is to *identify the training, aids/tools, and data needed to solve deception planning problems*. The second use of the framework is to *guide the application and development of new scientific and technological information* into the deception domain. The third use of the deception framework is to support *integration of new policies and doctrine*. The fourth use of the framework is to *guide and integrate the development and acquisition of resources* for deception planning. All four uses underscore the integrative nature of the deception framework and its value for the different aspects of battlefield deception. This report is focused primarily on the first use -- assisting the deception planner in construction of effective deception plans.

The deception framework is composed of two parts. The first part is a taxonomy of terms, concepts, and components relating to deception. This taxonomy provides the language with which to describe deception problems and their solutions. Using concepts defined in the taxonomy, the second part of the framework is a general process model of military decision making with deception embedded within this larger decision making context. Thus the framework is represented as a composite abstract object, comprising a *static* part and a *dynamic* part. The taxonomy (static) is described in this section and the decision making model (dynamic) in Section 3. The deception taxonomy is described in more detail in Zaklad, Moan, Zachary, and Knapp (1988).

Structure of the Deception Taxonomy

Tactical deception is a *problem-solving domain*, composed of the set of individual deception planning problems for which solutions must be generated. The process of problem solving is a complex cognitive phenomenon and over the last three decades, cognitive science has evolved a language for defining problem-solving domains. This formalism can provide the format for the defining taxonomy for tactical deception.

The cognitive definition of a problem-solving domain typically includes three separate components or specifications:

- *a goals specification* that breaks out and categorizes the kinds of ends or goals that domain problem-solvers try to achieve.
- *a means specification* that defines and classifies the means, or primitive actions that domain problem-solvers have available to achieve their ends.
- *a procedures specification* that defines the general process by which a specific means or set of means are selected, tailored, and applied in order to achieve a specific goal.

For the domain of tactical deception, the taxonomy takes for its third component the vulnerability parameters which specify and evaluate the deception procedures. Thus the deception taxonomy consists of:

- *deception goals* -- a taxonomy of the desired tactical end-states that are the goals of deception, such as changes in enemy timing, location or resource configuration, or changes in own-force understanding and control of enemy force intentions;
- *deception means* — a functional classification of the means available to achieve deception, including the tactical actions, psychological stratagems or materiel resources that may be used by the deception planner to achieve a deception end; and
- *vulnerability specification* — the concepts and parameters which must be considered in developing and evaluating different deception strategies, in the categories of nodes and decision makers, timing constraints and susceptibility.

Figure 1 shows the overall organization of the deception taxonomy.

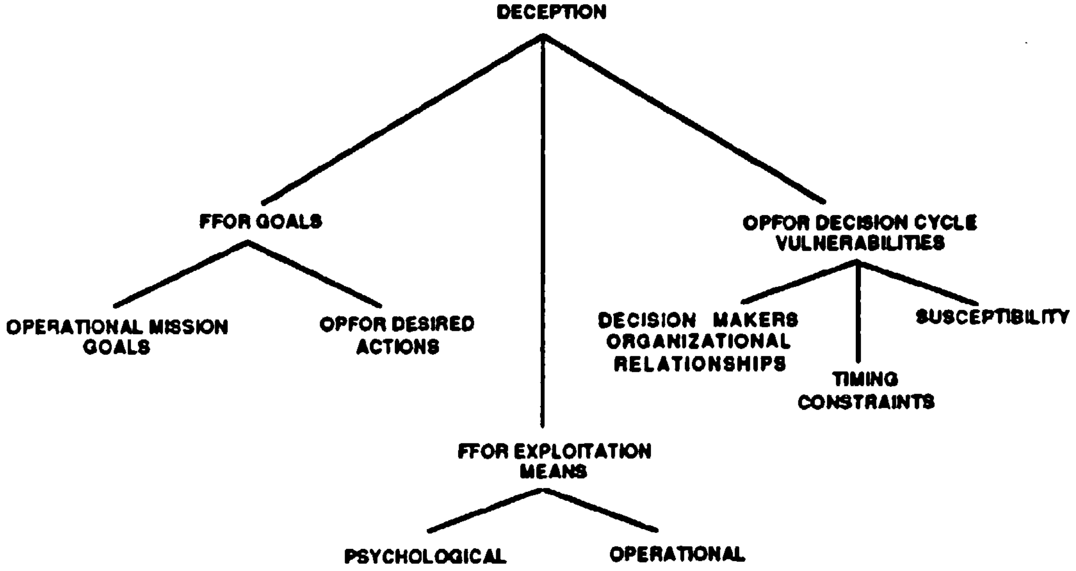


Figure 1. Overall organization of deception taxonomy

The FFOR (Friendly Force) Goals Component

This component defines what constitutes a "solution" to an individual deception problem, because the problem will be considered solved if a plan can be devised that accomplishes the goal. The goal taxonomy also describes the interrelationships among these possible goals and subgoals by placing them at various levels of analysis into a single hierarchical structure (see Figure 2).

Operational Mission Goals

The first checkpoint for deception is the identification of the overall operational mission goals. By noting the commander's mission objective (e.g., attack, defend, etc.) the mission goals are established to support this mission objective. The possible goals are: gain time (delay enemy action/reaction); reduce OPFOR assets; and, gain enemy (OPFOR) information. Any or a combination of these three may contribute invaluably to the commander's mission objective, and subsequently drive the nature of a deception plan -- what the FFOR would like to induce or reinforce in the enemy.

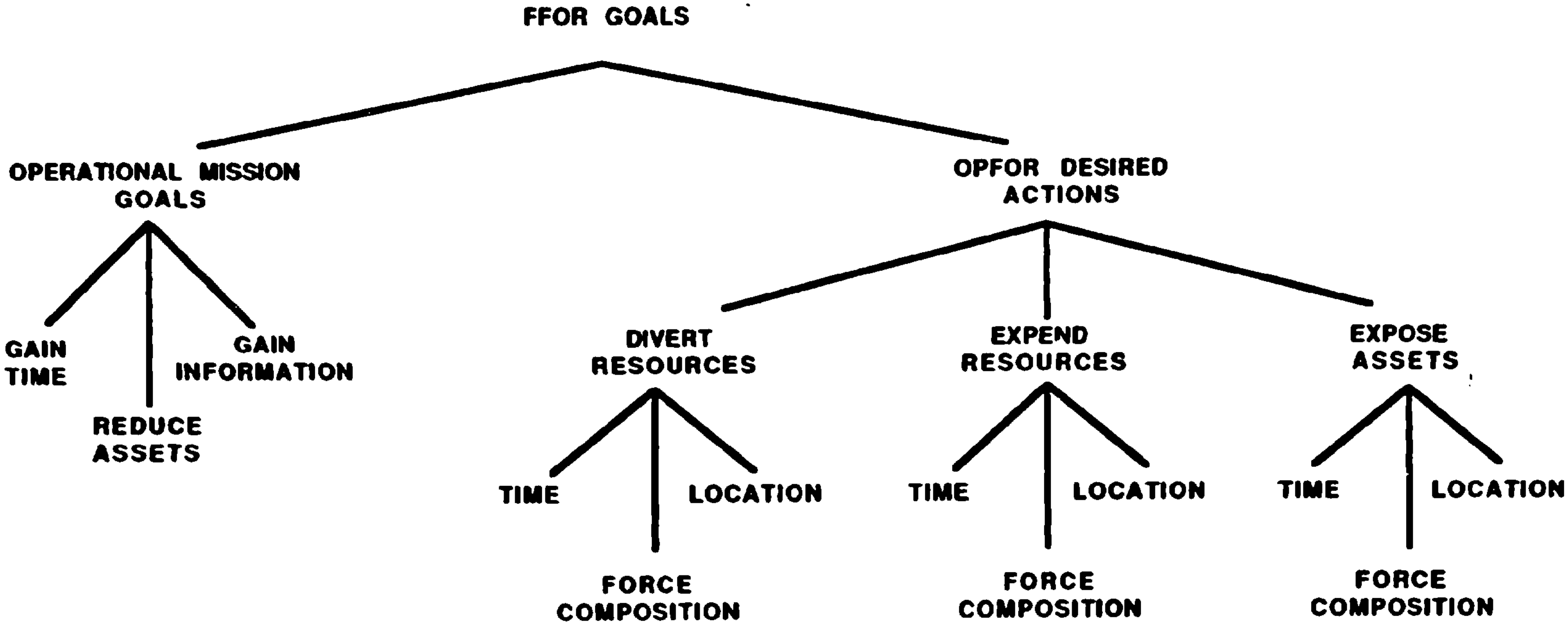


Figure 2. FFOR goals component

OPFOR Desired Actions

In concert with determination of the FFOR operational mission goal(s) is deduction of OPFOR desired tactical actions. This category includes most conventional deception activities, i.e., the playing out of the desired FFOR operation goal. Under this branch, the deception planner is trying to induce or reinforce the OPFOR commander, via a deception plan, to act in a manner more advantageous to the FFOR than in the absence of the FFOR deceptive measures. The OPFOR desired action branch thus supports the FFOR commander's ultimate goal of accomplishing his mission.

There are three major types or classes of tactical actions that the FFOR might like to reinforce (roughly corresponding to the operational mission goals): OPFOR divert resources, OPFOR expend resources, and OPFOR expose assets. Diverting and expending resources both refer to inducing the OPFOR to position or use personnel or materiel resources so that fewer resources will be available to meet a planned FFOR tactical action. Therefore the outcome distribution (spread of possible enemy courses of action) will be more favorable to FFOR. "Divert" refers to relocating OPFOR assets so that they will be out of position to respond to the FFOR planned action. "Expend" refers to the using up of expendable OPFOR assets with the same bottom line result. "Expose assets" means to gain useful information about OPFOR assets, based upon FFOR deceptive actions. All of these desired actions will need to be considered in relation to the time available for the deception, force composition, and location of enemy units.

FFOR Exploitation Means Component

The next major branch of the taxonomy identifies the various means available to the deception planner to achieve any or all of the goals identified above. The available means have been divided into two subcomponent (cf, Figure 1) branches. *Psychological means* include the various ways in which the "thought processes" of an OPFOR decision maker can be systematically manipulated. They define, in some sense, the available deception tactics or stratagems. However, like any tactic, they require other means to be implemented, thereby involving the other branch of the means component. The *operational means* define categories of actions which the FFOR could take to implement various of the psychological means. These categories include both FFOR maneuver and command and control activities. Also under the operational branch are the physical resources available to support or supplement the various operational actions. Resources include both standard, organic resources and deception-specific materiel. A deception plan will involve a complex combination of psychological tactics, and other supporting operational means.

Psychological Means

The first branch of the deception means component refers to psychological means and is depicted in Figure 3. Psychological means are the known avenues that the deception planner has to "get inside the OPFOR decision maker's head." In a very real sense, psychological means are the most critical means for deception. This is because tactical deception is essentially a psychological phenomenon, an attempt to manipulate the mental processes, or the decision making processes, of the enemy commander (Heuer, 1981). Not all mental manipulations are to be considered deception -- psychological operations (psyops) are psychological techniques directed against enemy troops, rather than against the decision maker or commander (e.g., exploiting prejudices). This part of the means taxonomy details the psychological stratagems, techniques, principles, and approaches to deceiving the OPFOR decision maker.

Figure 3 illustrates the highest level distinction in the psychological means, that between the *individual* and the *organizational.* This distinction refers to whether the particular technique or principle is primarily involved with influences on individual decision making or on group/organizational decision making. The proposed schema views tactical decision making as an individual cognitive process that occurs within some organizational context. This context provides the information needed for individual decisions, and the lines of authority and communication needed for the execution of these decisions. Individual and organizational decision making are seen to be both distinct and highly interrelated, as well as amenable to deception.

Individual Psychological Means. The individual segment of the psychological means structure is illustrated in the left half of Figure 3. The three categories of individual means are information processing, behavioral, and affective. More detailed discussion of the subbranches may be found in Zaklad, Moan, Zachary, and Knapp (1988).

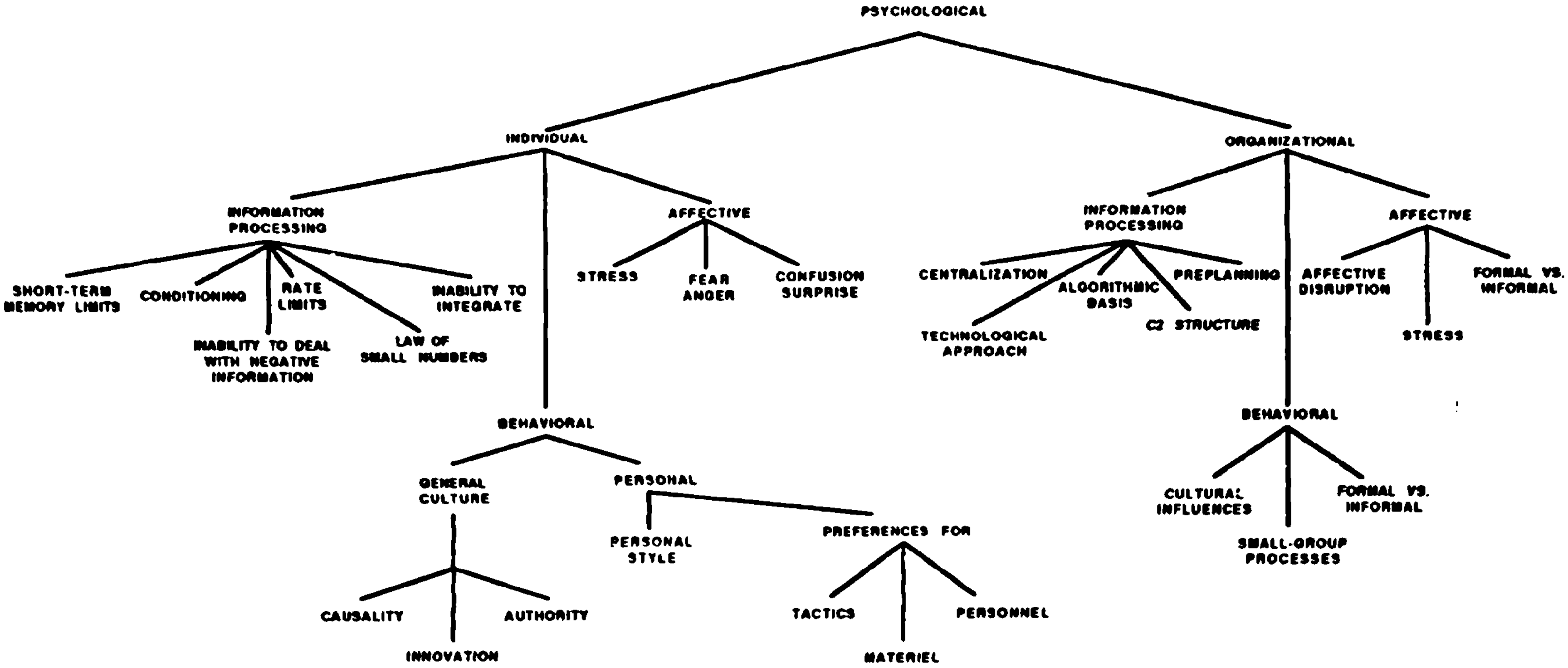


Figure 3. Psychological means component

Individual Information Processing Means. The individual information processing category is concerned with basic properties and limitations in human individual cognitive processing. All the factors described in this branch of psychological means deal with the human's attempts to make sense of the multitude of ambiguous and uncertain data available through sensory and cognitive mechanisms. It is in a very real sense a huge data reduction problem that confronts each of us -- to turn a mountain of incoming data into a manageable approximation of "what's out there" and "how things work." Several limiting aspects of human information processing have been experimentally demonstrated and discussed in the literature. Pylyshyn (1984) calls these aspects "architectural," in that they arise from the basic information processing mechanism which has close ties to the biology of cognition. These limiting factors create psychological opportunities for deception — the means problem solvers have to achieve their goals:

- Overload Short Term Memory Limits.
- Overload Information Processing Rate Limits.
- Appeal to the Law of Small Numbers.
- Apply Conditioning.
- Assume Inability to Integrate Information.
- Exploit the Inability to Deal With Negative Information.

Individual Behavioral Means. Individual behavioral means reflect points of view, perceptions, and strategies acquired during the lifetime of the decision maker. These are directed toward learned or acquired cognitive knowledge and processes that can be divided into two main classes of influence: cultural and personal. Cultural deception involves exploiting the "blinders" any culture places on the thought processes of individuals, while personal deception exploits the strong influence personal experiences have on the way a decision maker thinks and acts.

Individual Affective Means. Individual affective means refers to inducing strong negative emotions — such as fear, anger, surprise, and confusion — via tactical deception. These "gut" reactions are well known to reduce logical thinking ability and so can facilitate the OPFOR's belief in a deceptive operation. One of the important affective responses is stress, which should be used not as a single means for deception, but in conjunction with another action, e.g., a notional or actual attack.

Organizational Means. The second major class of psychological means are the organization means, which are depicted in the right half of Figure 3. These influences, in contrast to the individual means, act on the force decision maker through his entire organization. That is, organizational psychological means are derived from characteristics and vulnerabilities of the organizational contexts of individual decision makers. These also can be broken down into information processing, behavioral, and affective means.

Organizational information processing means. This category is analogous to the individual means. The information processing structure of an organization refers to that structure — functional components and their interrelationships — which is involved with the organization processing of information. This processing includes obtaining, interpreting, storing, and manipulating information for the purpose of making and implementing command decisions. Different organizations have different processing structures to accomplish their goals and objectives. These structures are sometimes explicitly designed to accomplish the goals; sometimes the structures evolve "naturally", without specific plans. Nevertheless, each information processing structure has certain strong points and vulnerabilities which derive directly from the structure itself, and define the organizational information processing means.

Organizational behavioral means. The second class of organization psychological means refers to exploitable characteristics that are learned rather than inherent in the structure. The organizational behavioral factors are cultural, small group processes, and formal versus informal processes. Cultural factors are analogous to the individual cultural factors — the distortions placed on organizational behavior by its surrounding culture. Small group processes refers to the body of knowledge of the dynamic functioning of small groups within larger organizations. The formal versus informal distinction applies to affective means as well as the behavioral since it can be used to create conflict and distrust, and disrupt the emotional well being of the enemy force.

Organizational affective means. The final category of organizational means refers to ways to induce disruptive or destructive emotional reactions into a tactical organization. Psyops is appropriately placed in this category, as in the individual branch. Organizational affective factors deal with the relationships among individuals within an organizational context. Using deception to introduce negative and distracting emotional dynamics into these relationships — including fear, anger, distrust, jealousy, despair — can be effective disrupting operations. Organizations can also be stressed just as individuals can. In the organization, stress relates to coordinative, cooperative, integrative activities; those that require interrelationship of roles and tasks. Building upon or enhancing naturally volatile dynamics would seem to be an effective way to utilize stress as a deceptive means. This approach also draws upon the formal versus informal distinction above, and the rivalries that often accompany it. Similarly, accentuating the competition for limited resources (e.g., multiple simultaneous attacks) can cause organization stress and performance decrements. Exploiting the discrepancies between formal and informal networks is an important deception means which may be behaviorally or affectively directed, but may be most effective when directed at both.

Operational Means

The operational means component is the second branch of FFOR exploitation means and is shown in Figure 4. This part of the means taxonomy details the operational/tactical actions, information control measures, and physical resources which might be used in conjunction with the psychological means to deceive the OPFOR decision maker(s).

Operational/Tactical Actions. Operational/tactical actions refer to the observable activities which comprise the planning, preparation and execution of courses of action at the operational sector and/or tactical levels. These activities are usually not deceptive in nature, but may be very effectively used toward such ends. They include the categories of logistics, maneuver, electronic warfare, signal and command control, air defense, other operations, fire support, deep battle, and engineer support.

Information Denial/Control Measures. Denial and control measures can best be analyzed by the sensor channel through which the OPFOR obtains the information. They can be classified into measures affecting the visual channel, the electronic-communications channel, the thermal channel, the olfactory channel, the sonic channel, or the physical channel. Information denial measures are procedures or actions applied to applicable sensor channels to inhibit the flow of salient information to the OPFOR over those channels. Information control measures are procedures or actions applied to sensor channels to regulate the quantity, nature, form, and timing to the OPFOR over those channels.

Physical Resource Means. The third branch of operational deception means is based upon specific physical resources. While psychological means may provide the basis or tactic for deception plans, and operational/tactical actions lay out the FFOR activities that are visible to the OPFOR, physical resources can be used in a variety of specific ways in deception operations to support or link together the larger pieces of the plan. Figure 4 shows the three main subcategories of deception resources: personnel; equipment; and deception materiel. Personnel are the military commander's most flexible and valuable asset; equipment is materiel that is organically assigned to the unit as part of its TO&E for purposes other than deception (such as sophisticated weapons systems); deception materiel is whatever equipment the commander has available specifically designed for deception , such as inflatable decoys or "black boxes".

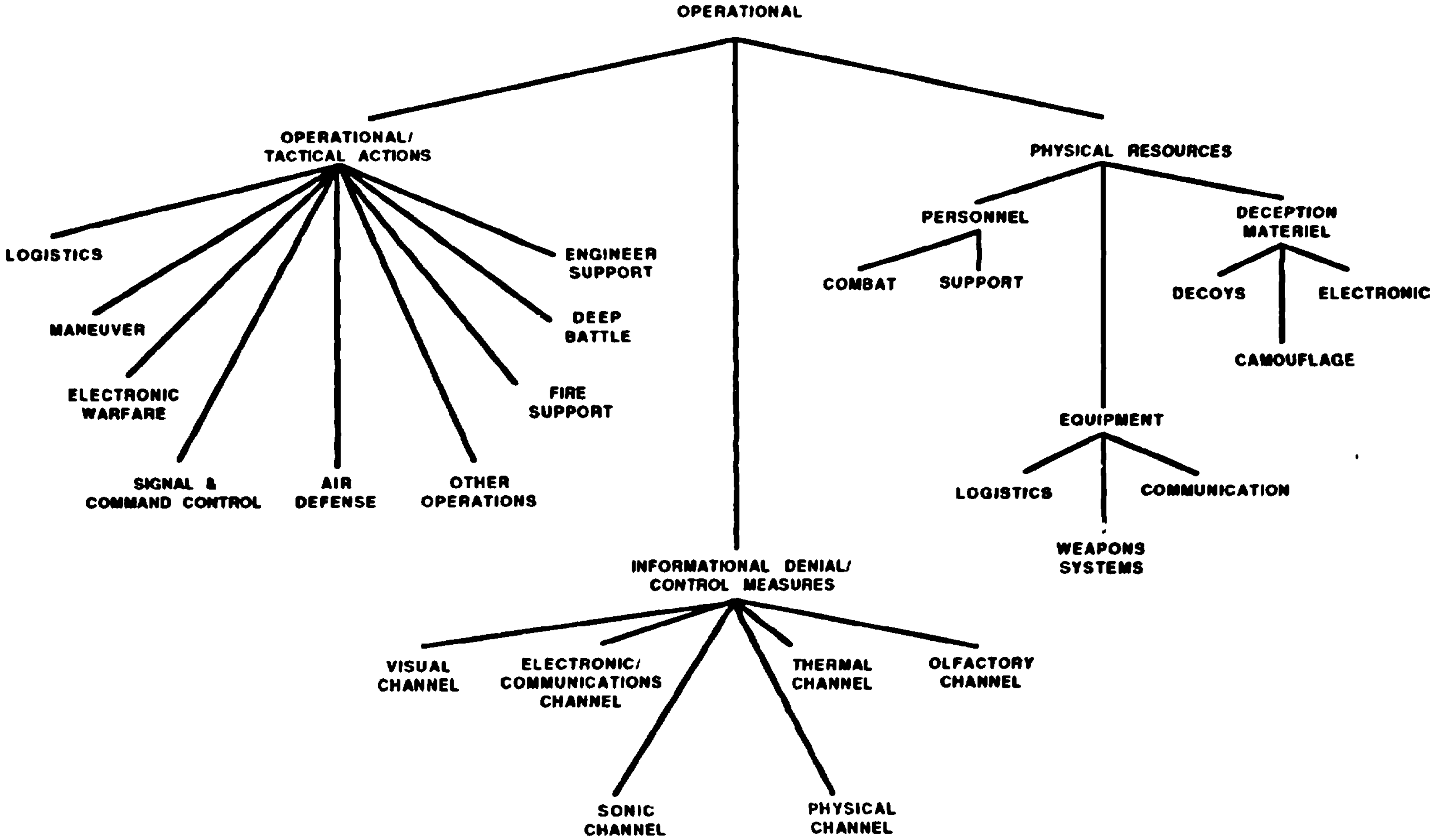


Figure 4. Operational means component

OPFOR Decision Cycle Vulnerabilities Component

The final taxonomy branch identifies the concepts and parameters which must be considered in developing and evaluating the effectiveness and feasibility of different deception strategies. This requires an examination of the OPFOR decision cycle by considering vulnerabilities related to decision makers, timing constraints, and susceptibility. The OPFOR decision cycle vulnerabilities component of the taxonomy is shown in Figure 5.

Decision Makers and Organization Structure

In order to fashion a specific plan in a particular area of operations/area of interest, the specific Order of Battle data and unit line and block charts of the OPFOR must be obtained. Beyond this, however, specific data relating to the actual decision makers, formal and informal means of communications, and information flow pathways must be identified. A network representation can be used to capture the information flow (paths of the network) and to identify the actual personnel who act on that information (nodes within the taxonomy) as well as specify their decision making roles (function of a node). Combining this network knowledge with data regarding the personnel characteristics and decision making characteristics within the command chain improves the likelihood that the deception means selected for operational situation will be successful.

Timing Constraints

Baseline data regarding timing of mission planning and execution phases of the OPFOR are a major driver of what deception plan can be accomplished and how effective it may be. Although it may be difficult to plot the exact timing of specific decision and execution phases for a given battlefield period, current intelligence should provide indicators of when opportune times for deception inputs exist and what time windows are available in which to execute various tactics. The derivation and representation of time windows involves physical, situational, and decision cycle pathways and flows. Physical timing constraints are those associated with movement, fires, communication, and resupply, and are based on the time it takes to carry out these actions. Situational timing constraints are either tactical or environmental, and include the time required to implement and execute tactical actions, and the time required to act under environmental conditions that prevail (terrain, weather, etc.). Decision cycle constraints are associated with the paths and steps in the OPFOR decision cycle, which includes time to pass information, to act on that information, as well as communication mode used.

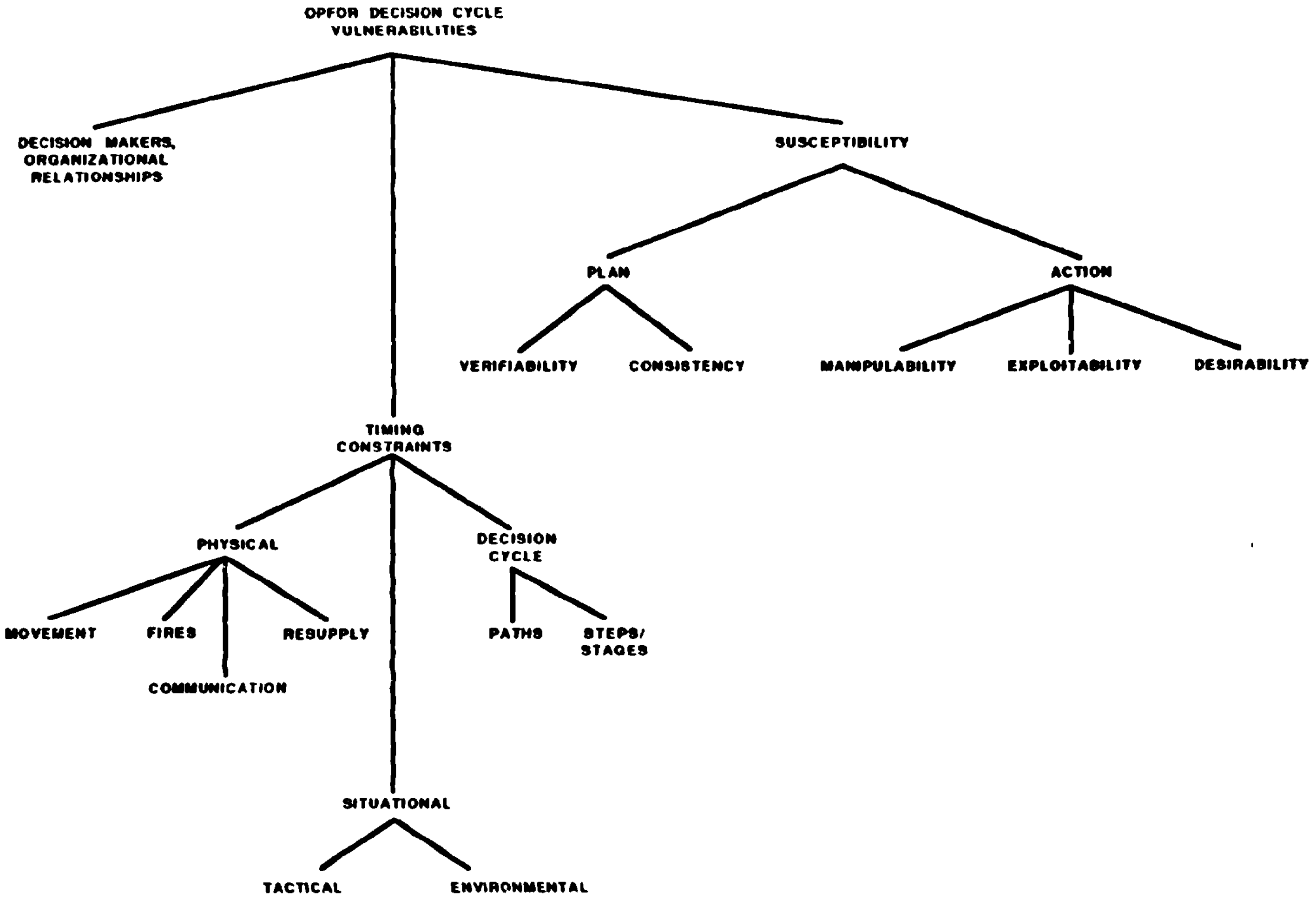


Figure 5. OPFOR decision cycle vulnerabilities component

Susceptibility

Susceptibility involves the FFOR capability to successfully construct and execute the deception plan, and whether plan execution will be compatible with the unfolding OPFOR decision cycle.

In the FFOR view, a wargaming process must occur which examines whether the planner has in fact identified the right information pathways, timing windows, and execution measures which will result in plan success. Important issues to be evaluated regarding the deception plan are:.

- verifiability, or how can the FFOR be dynamically aware of the extent of the plan's successful execution, and
- consistency, or how does the plan "hang together" with respect to past FFOR actions, the temporal course of notional events, activities of other and higher units, etc.

From the point of view of the OPFOR decision cycle, the concepts of manipulability, exploitability, and desirability are important. Manipulability is the extent that the OPFOR information paths and input channels are sensitive to deception data, that is, what channels are important to the OPFOR, and how they are used. Exploitability is the extent to which the FFOR can actually affect the selected information paths or input channels as they function in the OPFOR system. Desirability is the extent to which a particular OPFOR action is advantageous to the FFOR.

3. INFORMATION PROCESSES UNDERLYING BATTLEFIELD DECEPTION

A major conceptual question in analyzing, modeling, and aiding the battlefield deception process is how to bound the problem. From one viewpoint, deception can be viewed as a cognitive phenomenon. In this view, deception is a process by which a commander of one force causes the commander of another to make a specific decision or establish a certain belief about the battlefield. The purpose of deception, however is ultimately *behavioral*, not cognitive. That is, the commander performing the deception is interested ultimately in what the opposing commander does and not what he thinks or perceives. The opposing commander's beliefs and decisions are only a means to an end. The behavioral viewpoint sees deception as a process by which the commander of one force takes some action that leads the commander of another force to take (or avoid) some other specific action. This view can, in fact, subsume the cognitive view. It does this simply by noting that the actions of both commanders are based on goal-driven cognitive processes.

While this behavioral view of deception may be adequate for simple situations such as games (e.g. poker or chess) where two individuals attempt to deceive each other, it is still too narrowly bounded for the battlefield. In a military environment, the commander directs, rather than performs, action. The actual actions are performed by individuals within large organizations and constrained by factors of terrain, weather, equipment, command and control systems, intelligence gathering and processing capabilities, etc. Thus, a commander cannot take a deceptive action without:

- drawing limited resources away from some other key activities of his force;
- using the channels and means of command and control that are already at his disposal;
- continuing most or all ongoing activities needed to resupply, maneuver, and control his force for its main both purposes; and
- understanding how the action can and will be perceived by the opposing commander, through the filter of his organization's information gathering and processing structure.

This leads to a viewpoint of deception that is primarily *organizational*. The FFOR takes a set of actions, as directed by its commander and constrained by its environment and organization, which is intended to lead an OPFOR to take a corresponding set of actions that are somehow *favorable* to the FFOR. The space of FFOR actions is constrained by its organizational structure and information processes, just as the space of OPFOR responses is constrained by its organizational structure and information processes.

Each of these various viewpoints on deception — the cognitive, the behavioral, and the organizational — was explored as a possible framework candidate during the early phases of this project to identify its potential payoff for supporting the battlefield deception needs of the Army, as well its attendant costs. In the end, it was concluded that the constraints of the command, control, communications and intelligence processes were critical to the real-world application of deception. Because these constraints come into play only when deception is viewed organizationally, it was decided to focus on deception at the organizational level. The first step in applying this viewpoint was to develop a model of organizational information processing in military systems, and use this to construct a model of deception. These models constitute the second part of the psychological framework for deception.

Organizational Information Processes

There are numerous models of organizational dynamics in the research literature. A review of these models pointed out two requirements of this project that were not met by any existing model:

- the model had to deal explicitly with the command-and-control and echelon principles that form the basis of military decision making and action, and
- the model had to be expressed in information processing terms so that the links between decision making and behavior could be clearly traced.

As a result, a new model of organizational information processes was developed by integrating theories and partial models from both organizational and cognitive science, as encouraged by interdisciplinary researchers such as Malone (1989).

This model draws from cognitive decompositions of the process by which individuals process sensory data and make decisions to generate and take actions. These decompositions generally decompose the process into stages that correspond to subsystems or sub-processes. Card, Moran and Newell (1983), for example, break the process into perceptual, cognitive, and motor subsystems in their Model Human Processor architecture. Wohl (1981) uses a similar decomposition into stages of stimulus, hypothesis formation, option generation, and response in his SHOR model. The current model draws on organizational science theories of both general and military organizations. The general theory of functional decompositions of organizations as presented in various sources provided a conceptual bridge between the functional decomposition of cognitive processes (as cited above) and a class of organizational structures known as functionally-organized structures. A more specific model of military organizational processes was found in the Headquarters Effectiveness Assessment Tool or HEAT developed (see DSI, 1983,1984). HEAT was a process-evaluation tool that was built around a functional model of how information is processed in a military C2 structure.

The basic model of information processing in military organizations deals with the flow of information at a given echelon. Within any echelon, the processing is decomposed into five general steps or functions:

- *Sense* — collect raw information from the environment
- *Analyze and Integrate* — develop a battle situation description and interpretation by fusing sensed information and applying corporate and individual knowledge
- *Evaluate and Decide* — make decisions about a course of action based on evaluation of the situational data and situational goals (including orders from higher echelons)
- *Plan and Supervise Course of Action* — construct a plan to carry out the decided course of action, and modify/revise that plan during its actual execution based on the success/failure of individual actions
- *Act* — carry out and control individual battlefield or background actions as part of the overall plan

In psychological terms, the first function (sense) corresponds to sensory/perceptual stages of information processing, the second through fourth correspond to the cognitive stages, and the last (act) corresponds to motor level actions. These five functions are linked in a simple serial model and depicted in Figure 6. This figure organizes these actions into a pyramid to reflect their relative distance from the organization's environment, which is implicitly represented at the bottom of the figure.

Figure 6, however, represents only a basic or skeletal structure of an appropriate model for this effort. Specific factors of military organization had to be introduced to enhance the realism of the basic model. Each function in Figure 6 can be readily associated with one or more specific C3I (command, control, communications and intelligence) function in Army doctrinal organization. The intelligence function is associated with Sensing and Analysis and Interpretation, the operations function is associated with Planning & Supervising Course of Action and with Action, as is the logistics function. Command functions are associated with the Evaluate and Decide Function.

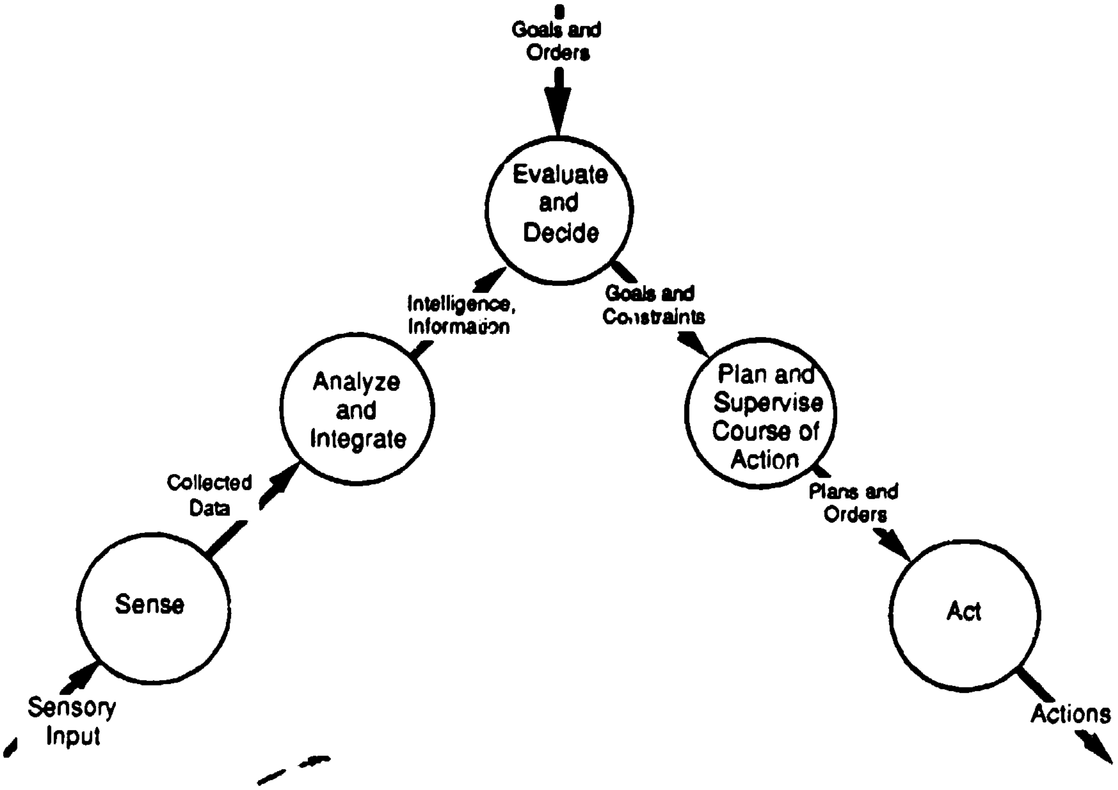


Figure 6. Basic action generation model

Single Force Decision Making

The realities of real military operations dictate many interconnections between the functions depicted in Figure 6. For example, feedback on the success/failure of actions and plans must be provided from the Act function to the Plan and Supervise function, and between the Plan and Supervise function and the Evaluate and Decide function. Similarly, requirements for future information needs must be sent from the Evaluate and Decide function to the Analyze and Integrate function,and from the Analyze and Integrate function to the Sense function, so that the information needed for successful completion of a decided course of action will be obtained. Figure 7 shows a more complete model of the intra-echelon action generation process, which incorporates these (and other) internal information flows. This model was used as the basis for understanding how information flowed from sensing to action generation within a given echelon.

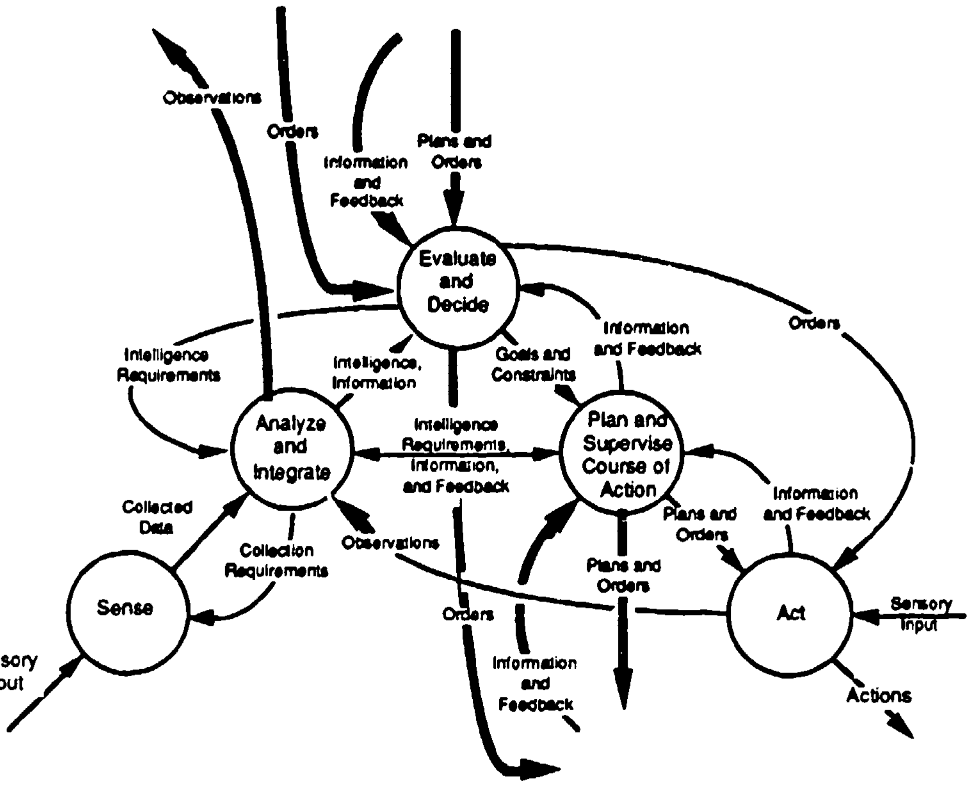


Figure 7. Intra-echelon action generation process model

The model shown in Figure 7 provides a reasonably detailed representation of the process that must be manipulated through a deception plan at a given echelon. There are two more levels of detail that must be considered, however, in making this model complete. The first is the role of echelon. In military organizations, the flow of command and control information and the action generation process operates both within given echelons and across echelons simultaneously. Specific functional areas such artillery or armor, must be coordinated across units of a given echelon and integrated into a higher-level course of action. This is done by cross-echelon command and control. Figure 8 shows how the basic action generation process links across echelons to model the coordinated actions of units operating at multiple echelons of a given fighting force. It should be noted that only one unit at each echelon is shown in Figure 8 for simplicity.

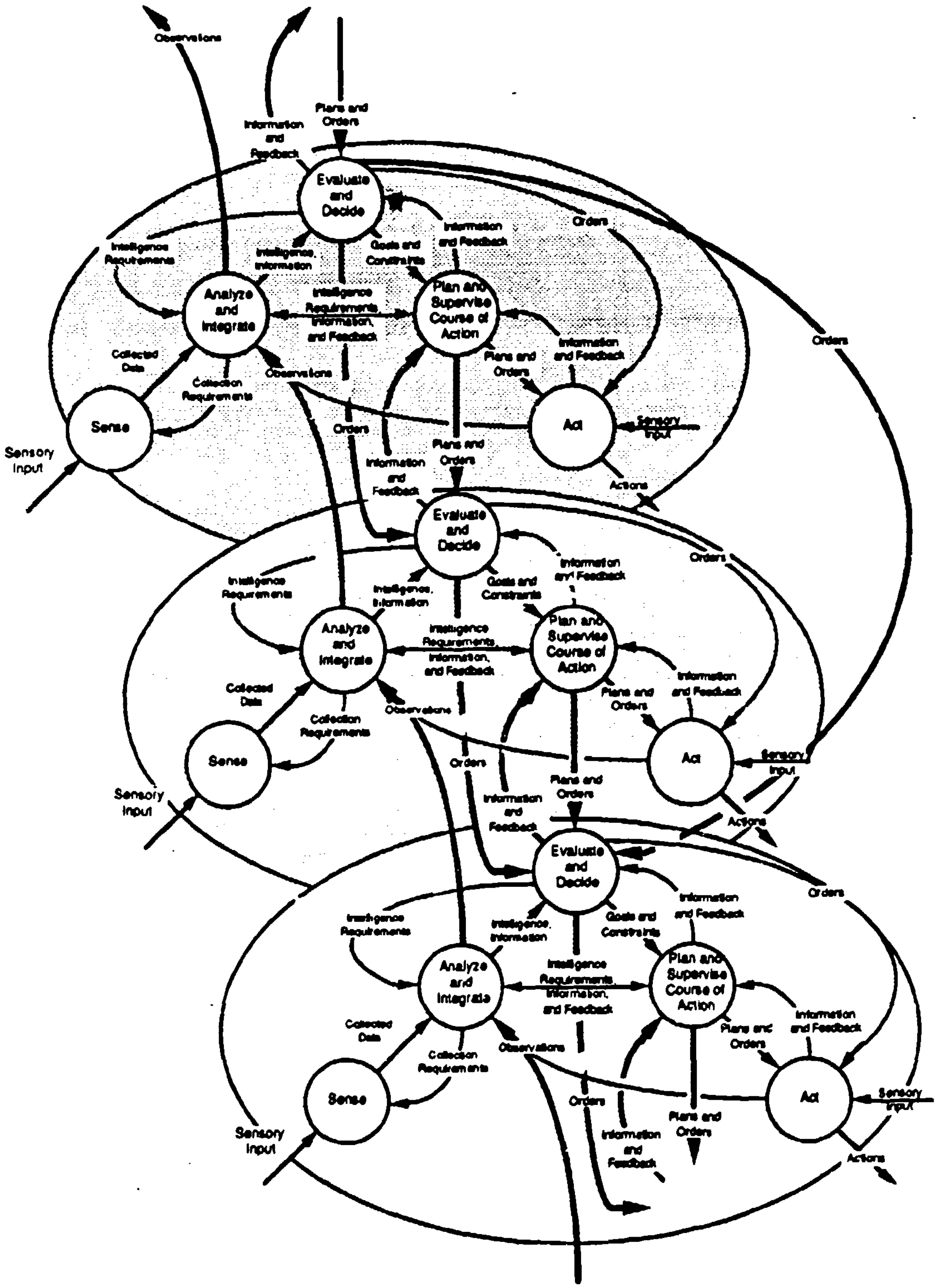


Figure 8. Inter-echelon action generation process

Obviously, if the unit represented at the top of Figure 8 has three major subordinate commands, and each of them also has three major subordinate commands, the complexity of the interconnections is significantly greater than that displayed in this figure.

Force on Force Decision Making

The final level of detail in the action generation process model is to view the model as a pair of reflexive models, one representing the FFOR and one representing the OPFOR. In this view, the FFOR receives sensory inputs that include some view of the current actions of the OPFOR. These (intelligence) data are analyzed and evaluated by the FFOR in determining the FFOR course of action (which may simply be to continue the previously planned Course of Action). As the FFOR implements its selected course of action, its actions are viewed (at least in part) by the OPFOR and used in an analogous manner in the analysis and generation of its (OPFOR) actions. It should also be noted that each force senses the other not merely through its formal sensing or intelligence channels. The actual contact of forces, which occurs at the levels of FFOR and OPFOR functions, provides another major channel for sensing. Thus, the FFOR actions can be viewed as feeding into the OPFOR Sensing and action functions, just as the OPFOR actions can be viewed as feeding into the FFOR sensing and the FFOR action functions. This structure is pictured in Figure 9 for a given echelon, with the inter-force interactions shown as dashed lines. The final elaboration would expand this inter-force intra-echelon view to a multi-echelon view, although the resulting model is too complex to picture.

Figure 9 helps define how battlefield deception occurs. The FFOR decision maker determines what the OPFOR is or may be doing from the various sensing and analysis and integration functions, and decides to deceive the OPFOR into taking a different course of action (or inappropriately persisting on the present course of action). In either case, a deception plan must be constructed at the plan and supervise level, and then implemented at the action level. This plan must be designed so that it its actions are in fact viewed by the appropriate sensing mechanisms of the OPFOR, and so that the analysis and interpretation of these sensings will lead to a specific (but ultimately untrue) situation description at the analysis and the evaluation levels. The OPFOR commander, then, presented with this situation description, makes a seemingly appropriate decision and selects a course of action, which is then planned in detail , supervised and carried out by the planning and supervision and the action functions.

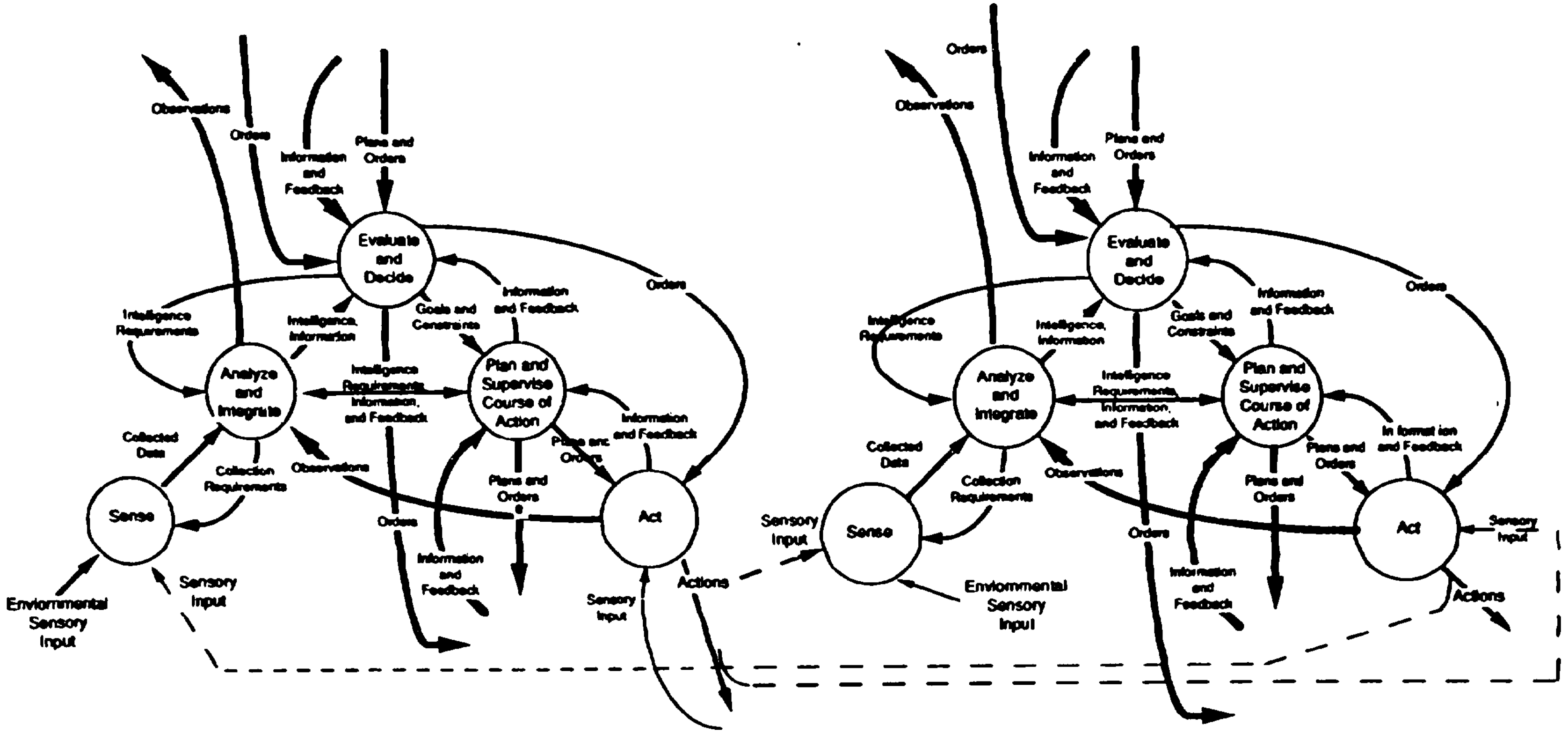


Figure 9. Interacting command and control organizations

This model framed the requirements for the remainder of this study. It made clear certain distinctions and concepts about deception planning that were otherwise absent. For example, the OPFOR can be seen as vulnerable to deception only with regard to those input (i.e. sensing) data to which the OPFOR decision cycle is sensitive. If the OPFOR can or does not sense a particular piece of information, or if that information can or does not affect the decision cycle, then the OPFOR is not vulnerable to being deceived with such information. Conversely, the FFOR can not exploit a vulnerability if the FFOR can not systematically manipulate a type of information to which the OPFOR decision cycle is vulnerable.

Given these definitions and the analysis which follows from them, the model then served to define the requirements for the remainder of this effort. The generic model in Figure 9 first had to be related to specific models of how the US/NATO (FFOR) and the Warsaw Pact (OPFOR) carried out the various functions in the model. Second, the standard "evaluate and decide" options of the NATO/Warsaw Pact FFOR/OPFOR had to be analyzed and modeled so that exploitable vulnerabilities in the OPFOR could be identified. And third, a procedure for developing deception plans that could in fact exploit these vulnerabilities had to be defined, and supported with detailed planning aids and tools.

A comparative overview of the FFOR and OPFOR decision-making cycles for deception planning reveals a major difference between the two forces regarding their internal information flow: FFOR information flows both vertically and horizontally between echelons, making it more interactive; OPFOR information has a more centralized, vertical focus. As a result of this centralization, horizontal coordination and knowledge within an OPFOR echelon is often minimal and thus may be exploited by FFOR deception. Aside from this centralization, there are other exploitable factors resulting from differences in the FFOR and OPFOR decision cycles. Thus, understanding of the organizational structures and decision making approaches taken by each force is an important initial step in acquiring knowledge for application to a deception planning operation. A detailed comparative overview is found in Moan, Broz et al, 1989.

4. COGNITIVE SCIENCE ENHANCEMENT OF THE DECEPTION PLANNING PROCESS

The process of problem solving is a complex cognitive phenomenon, and one that has been extensively researched in cognitive psychology and cognitive science. Problem solving itself may be defined as a sequence of actions that carries a system from an initial state (or current situation) into a goal state (or desired situation). Such a "successful" sequence of actions is called a *solution*. Cognitive studies of problem solving have shown that there is a broad set of solution procedures that may be applied to any problem solving domain, including those of the battlefield (Newell & Simon, 1972; Simon, 1981; Amarel, 1981,1982). This section uses concepts of cognitive science to analyze, elaborate, and enhance the current doctrinal deception planning process.

This section first defines key cognitive terminology, then lays out the current deception planning process as set forth in Field Manual FM 90-2. Certain cognitive science concepts are applied to this process, resulting in a detailed, multi-faceted deception plan approach for use by the US Army. This *enhancement* of the deception planning process includes its division into two complementary phases — the constructive and the derivational — each of which is elaborated upon in this section.

Current Deception Planning Solution Procedures

The procedures that are currently mandated for deception planning are presented in FM 90-2, and provide a number of complementary viewpoints:

- overarching maxims and guidelines;
- general doctrine on the role of deception at various levels of operations;
- general steps in the planning process; and
- guidelines on the use of specific classes of means/material.

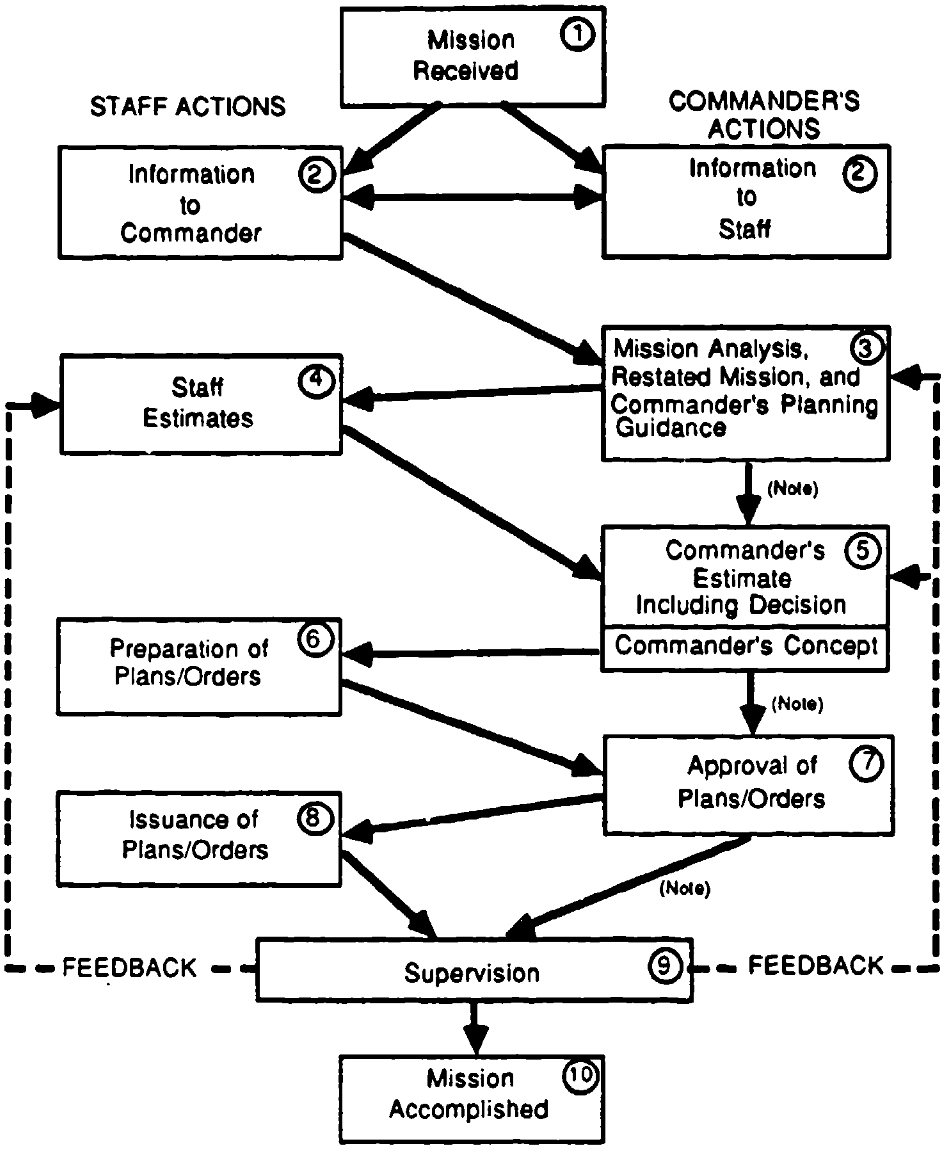
Each of these discussions is relatively complete, but there is little integration of the elements of deception planning. For present purposes, the most relevant items are the maxims and guidelines, general doctrine, and general steps. A similar approach to deception planning is taken by the U.S. Air Force Special Operations School (U.S. Air Force, 1989).

Deception as a Part of Overall Operations Planning

To understand deception planning, it is necessary to first look at overall operations planning. As a component of the complete operations plan, the deception plan is constructed in parallel fashion to the other components. The difficulty of the planning problem, the required security, and the availability of time and other planning resources will influence the degree to which the commander specifies the plan or delegates planning details to the deception cell. Figure 10 illustrates the general operational planning steps for the commander and staff:

- Step 1 — Commander receives or deduces mission.
- Step 2 — Staff considers mission constraints and own capabilities
- Step 3 — Commander completes mission analysis and issues planning guidance.
- Step 4 — Staff formulates estimates.
- Step 5 — Commander formulates estimates and issues commander's concept.
- Step 6.— Staff prepares plans.
- Step 7 — Commander approves plans.
- Step 8 — Staff issues orders.
- Step 9 — Commander and staff supervise execution of orders.

The iterative nature of the planning process is reflected in these steps. A first, quick pass through the planning problem occurs in Steps 1 through 3 and a second, more detailed examination occurs in Steps 4 through 6. The detailed plan/orders are finally produced in Steps 7 through 9. Each of these sequences has a similar structure. First, the problem is analyzed and defined; second, plans at a given level of grain are constructed; and third, the plans are executed or transferred for a more detailed development. Many of the same tasks and sub-processes are employed in each iteration, but at different levels of detail. This same characteristic obtains for the deception plan -- it is iteratively derived, with each succeeding pass more detailed.


Mission Received 1
STAFF ACTIONS
COMMANDER'S ACTIONS
Information to Commander 2
Information to Staff 2
Mission Analysis, Restated Mission, and Commander's Planning Guidance 3
Staff Estimates 4
(Note)
Commander's Estimate Including Decision 5
Commander's Concept
Preparation of Plans/Orders 6
(Note)
Approval of Plans/Orders 7
Issuance of Plans/Orders 8
(Note)
FEEDBACK
Supervision 9
FEEDBACK
Mission Accomplished 10

NOTE: In time-critical situations, the commander may be forced to complete his estimate based on his personal knowledge of the situation and issue oral orders to his subordinate units.

Figure 10. Intra-echelon decision making process

Current Deception Planning Steps

The deception planning process unfolds as a part of the operational planning process as described above. Figure 11 (taken directly from FM 90-2) shows the general steps in current deception planning.

Eight generic planning steps that are essential to deception plan construction have been abstracted from FM 90-2. Six of these — evaluate situation, determine deception objective, determine desired perception, establish story, develop plan, and execute and monitor — are listed explicitly in the Field Manual. In addition, two other logically required generic steps have been identified — to identify the deception target and develop the deception target. These are not explicitly identified as separate steps in FM 90-2.

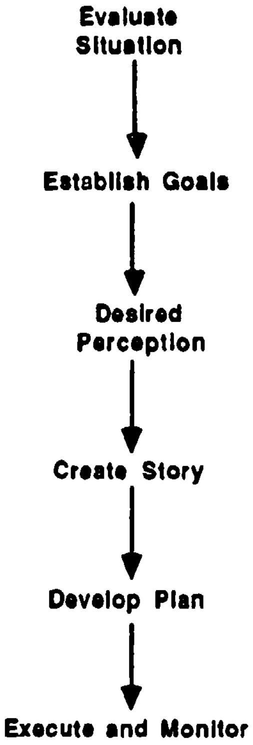


Figure 11. Current deception planning process (FM 90-2).

These steps are defined in terms of *objectives* or what the planner seeks to accomplish at the end of the step, rather than in terms of the process by which it is accomplished. Any or all of them may be pursued in varying detail according to the stage of the operational planning process described above and the characteristics of the problem. The eight steps each with its associated objective are shown in Figure 12:

- *Evaluate situation* — A deception plan can be developed only if the planner understands the current situation.
- *Determine deception objective* — The planner receives a mission from his commander.

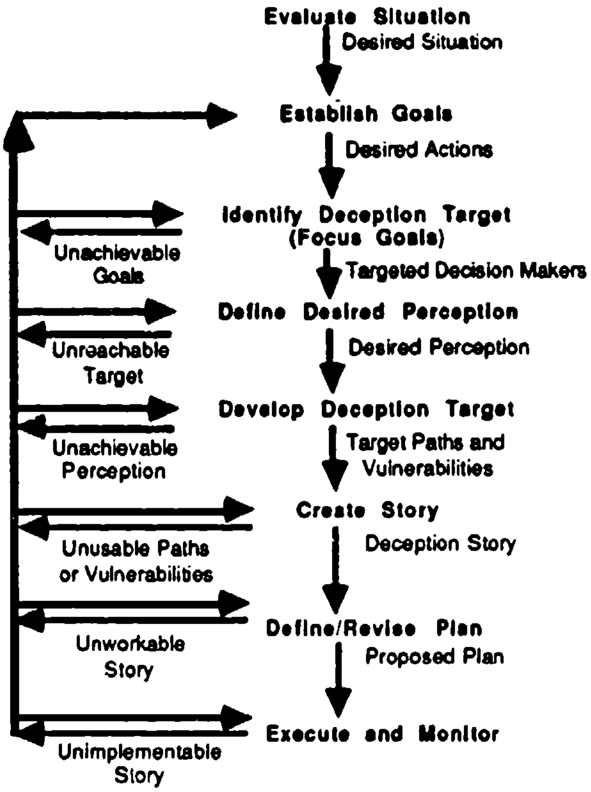


Figure 12. Overall deception planning process

- *Identify deception target* — Once a specific deception goal has been selected, the planner then defines the target of the deception plan. He determines which specific decision maker(s) must be affected, if the goal is to be obtained.

- *Determine desired perception* — In this step, the planner projects the specific deception goal onto the targeted decision maker(s).

- *Develop deception target* — Before proceeding to develop the outline or details of a specific plan to engineer the desired perceptions on the target decision maker, the planner develops more information about the target and its position in the OPFOR.

- *Establish story.*— In this step, the planner makes a first-pass or coarse-grained plan.

- *Develop plan* — In this next-to-last step in the process, the detailed sequence of deception means is gathered, organized, and interrelated to yield a detailed plan.

- *Execute and monitor*-- In this final step, the plan is executed and the results monitored and evaluated.

Solution Procedures in the Deception Domain

There are two relatively integrated literatures relating to deception and deception planning: the extensive writings on *Maskirovka* by Soviet sources; and the smaller Western literature on deception. Both bodies of literature focus mainly on analyses of specific operations, and the reasons they succeeded or failed. Analyses by Glantz (1985), the CIA reviews (ORD, 1978, 1981, 1982), and many of the Soviet sources fall into this category. From these analyses, generalizations have been drawn that can be applied to other situations (ORD, 1981; Handel, 1982). In particular the ORD work draws a number of principles or maxims that represent useful knowledge about the planning process; these maxims are focused at the level of individual pieces or attributes of deception plans. They suggest when a certain technique should or should not be used, or when a deception plan should have a certain feature. They represent planning knowledge that can be used to *produce* a solution, and thus suggest a *constructive* solution.

There are other aspects to the literature that argue for a more derivational approach. FM 90-2 and other doctrinal literature (e.g., U.S. Air Force, 1989) discuss such concepts as "demonstrations, feints, ruses, displays." However, a demonstration, a feint, a ruse, or a display cannot be considered to constitute an entire deception plan in and of itself. These concepts really represent partial solutions or larger-scale building blocks of a deception operation that are more suggestive of a derivational solution procedure. It is important to note that these more derivational partial solutions apply to FFOR operations, while the more constructive heuristics discussed above apply to the OPFOR. The implication is clear — **there is more knowledge available on how to organize and control our forces to project a deception story to the OPFOR than there is knowledge about how to figure out what 'story' to project.**

This result suggests that a two-part solution procedure for deception planning is necessary. The first part should be highly constructive, in which a deception story is built. The second part should be somewhat derivational, using a hypothesize-and-revise approach in which chunks of partial solutions are adapted to develop a detailed plan to project the deception story.

The enhanced deception planning process, shown in Figure 13, was defined with these two parts in mind. Initially, the current planning procedure is analyzed and abstracted to its basic structure. Then that structure is modified to reflect places and ways in which more focused knowledge such as ORD's heuristics can be inserted into the procedure. The derivational or adaptive part is defined following the constructive. A hypothesize-and-revise process is

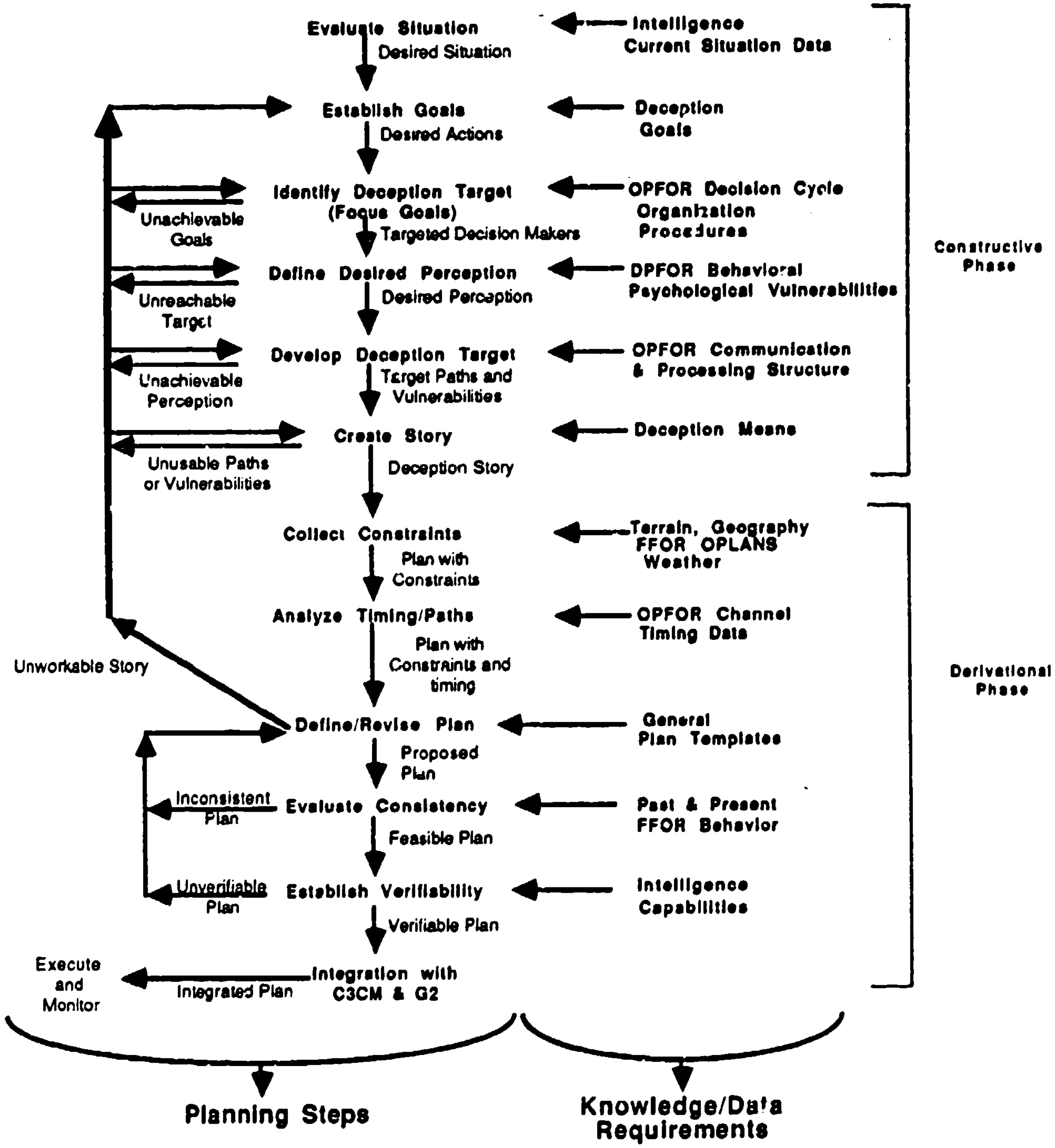


Figure 13. Enhanced deception planning procedure

delineated in which a partial solution is first adapted, and then revised using various heuristics. An additional feature of this representation of deception planning is the right-hand column, which specifies the data and knowledge needed by the planner in order to accomplish each step.

The Constructive Phase of the Deception Planning Process

Draft FM 90-2 provides only the barest skeleton of a planning process and does not suggest a specific problem-solving procedure by which any of the above steps can be accomplished. The constructive phase of the solution procedure seen in the upper part of Figure 13 attempts to do this by building a deception story.

The steps listed in the figure are pursued sequentially, beginning with an evaluation of the situation and ending with the completed deception story. At each step, a piece of the story is created. The first step results in a situation that the deception planner desires to create. In the next step, the planner works backward from this desired situation to determine which OPFOR actions lead to the desired situation. These desired actions become the objective of the deception operation. ORD's (1981) "rule of multiple forms of surprise" suggests a heuristic for this step: **find and keep a set of alternative goals that could yield the desired situation, and propagate these alternatives through the rest of the process.** There are two reasons behind this heuristic. First, some of these goals may later prove unachievable. Second, and more important, the deception story should not "put all its eggs in one basket". The planner should anticipate that some aspects of the deception plan may fail in execution, and consequently build alternatives into the plan.

The goals are focused on specific OPFOR decision makers in the next step of the process. There are two possible outcomes of this step. Although not always possible, the desired outcome is identification of one or more decision makers who are in a position to take the desired OPFOR actions. There may be no decision maker in the sphere of the operation who is able to do this. Alternatively, the desired OPFOR actions may require recourse to a higher OPFOR authority or a time frame that is beyond the scope of the deception operation. In such cases, the deception goals are determined to be unachievable, and the process returns to the previous step in order toredefine the goals of the operation. A large amount of knowledge about the OPFOR organization, decision cycle, and procedures is needed to effectively carry out this step.

When a specific set of decision makers can be targeted, the process proceeds to the next step. Here, the planner continues to reason backward by defining the perceptions or beliefs that the targeted OPFOR decision makers would have to maintain for them to take the desired actions. Here again, two outcomes are possible. In the desired case, the planner can define one or more perceptions which would lead to the desired actions. Alternatively, the planner may be unable to define a perception that would lead the targeted decision maker to take the desired action. In this case, the target is considered to be unreachable, and the process returns to a previous step to redefine the goals or to retarget the goals on different decision makers. This step involves the use of knowledge about the behavioral and psychological vulnerabilities of OPFOR decision makers to deception.

When a desired perception can be defined, the deception planner proceeds to find paths and channels by which the targeted decision makers can be reached and their perceptions manipulated. There are two parts to this step: (1) paths of access must be identified , and (2) their susceptibility to systematic manipulation by the FFOR must be verified. Here again two outcomes are possible. The planner will ideally identify a set of channels by which information to manipulate the targeted decision maker's perceptions can be conveyed. If such channels cannot be defined, then the desired perception must be deemed unachievable, and either the goals, targets, or desired perceptions must be reconsidered. Again, substantial knowledge about the OPFOR is needed to identify paths to the targeted decision maker and to assess the vulnerability of these paths. This is called *pathfinding*.

Pathfinding, which requires a great deal of knowledge about the intelligence collection, communication, and analysis systems of the OPFOR, is a means for deception target development which builds on OPFOR decision making vulnerabilities. These are the vulnerabilities implicit in the analyses of the information environments in which the targeted decision makers are working. They are also implicit in the statement of the desired perceptions which they must hold if they are to execute the desired actions. Pathfinding attacks the targeted decision makers by attempting to find potential ways to manipulate their decision environment (via their available intelligence and knowledge). The purposes of this manipulation is to significantly increase chances that the OPFOR will execute the desired actions and thus bring about the desired situation for the FFOR.

The final step of this constructive portion of the solution procedure is directed toward integration and elaboration of the results of the previous steps to create a complete deception story. Up to this point, the solution process has worked backward from the goal state: linking it first to specific decision makers; then to desired perceptions; and finally to channels of access to those decision maker. This step links this chain of backward reasoning with the current situation by defining a set of events that begin with the present configuration of forces and information and ends with the OPFOR taking the desired action and creating the desired situation. The result is a deception story that will then be turned into a full plan in the second portion of the solution process. Alternatively, if no story can be constructed, then the identified channels to the targeted decision maker are unusable. In that case, the process must return to a previous step to find different channels, different perceptions, different targets, or different desired actions.

The constructive part of the process ends with the deception planner beginning a second phase of planning in which he translates the deception story into a specific set of actions and orders.

The Derivational Phase of the Deception Planning Process

Now that these bases for the deception planning process have been discussed, a more detailed examination of each of the steps involved can be made -- the derivational phase pictured in the lower half of Figure 13. The deception planner begins the planning process with a proposed deception story, complete with an OPFOR deception target and paths to that target. All of this is based on a specific deception objective and desired target perception. Before a specific plan is developed, however, two steps are taken to gather data for the plan development process. These are collecting constraints and analyzing the timing requirements of the deception story. First, the planner must identify the operational constraints under which the plan will be executed. These include specific resources which will or won't be available for the plan; constraints which the local geography, terrain and weather impose on maneuver; timing, positioning, maneuver and fire requirements of the main OPLAN which may constrain the deception plan; and timing and resource limits for the deception planning process itself. These are all factors which will be used to adapt a plan template to the specific conditions of the operation at hand. Ideally, the planner will have a checklist to identify the specific constraint information that should be collected. The result of this step is the original proposed deception story plus a set of constraints within which it must be put into operation. These constraints can also come into play in the evaluation of any candidate deception plan.

The planner may then perform a more detailed analysis of the specific paths to the OPFOR target that are used in the deception story. Each sequence of paths or *channel* will have certain timing constraints and delays associated with it. For example a radio link may be manipulated instantaneously, but the report of the manipulation may be delayed by the radio operator before sending. The specific timing data form temporal constraints on the plan which implements the deception story. These constraints may also affect the plan's consistency and verifiability.

The main step in this part of the procedure is defining/revising the deception plan. Like any kind of operations plan, the deception plan requires details about specific units, times, locations, frequencies, and so on. It employs the concept contained in the deception story. In developing the initial candidate plan, the deception planner analyzes the deception story and identifies an existing or canned deception template which appears to meet approximately the requirements of the current deception story. These templates may have been built purely analytically, but more likely they wil, oe based on abstractions of past deception successes. After defining a plan template, the various constraints and timing details are factored into the template to adapt it to the current tactical situation-at-hand. Items such as specific unit assignments, frequency channels, and movement locations are assigned to the appropriate slots in the general plan template to build a specific plan. In the initial pass through this step, it is unlikely that a decision could be made that no workable plan could be constructed from the deception story. After one or more passes through the revision cycle, however, the planner may eventually decide that no revision of the plan could make it acceptable. The deception story may then be concluded as unworkable.

The candidate plan is then evaluated for its consistency once all the temporal and other constraints have been gathered. Separate evaluations should be sequentially made for its breadth, temporal, behavioral and external consistency. First, the consistency of information across the various paths to the OPFOR target should be evaluated, and inconsistencies noted and attached to the plan. The consistency of the unfolding story over time is evaluated next, again with inconsistencies noted. After that, the consistency of the overall plan with past FFOR operations should be evaluated. This evaluation, it should be noted, requires a substantial database of information on past tendencies, trends, and behaviors of the FFOR. Inconsistencies again are noted and appended to the plan. Finally, the consistancy of the plan with regard to other OPFOR operations must be evaluated, and inconsistencies noted.

The candidate plan is either judged inconsistent or found to be feasible after these four separate evaluations. If inconsistent, it is returned to the 'revise plan' step where the inconsistencies are analyzed and used to revise the plan. If feasible, the plan is subjected to one last evaluation step to establish its verifiability. In this last step, the planner analyzes the deception story to determine key points at which the OPFOR target must be affected. For each such point, the planner must identify what information could be used to tell whether or not the story was being accepted at that point. The deception plan is examined to see: (1) if a means of obtaining this verification is built into the plan; and (2) if this verification means can and will obtain the information needed to verify the story's success. The planner needs substantial knowledge of the intelligence capabilities of the various verification means included in the plan. If the verification is not included or if the planned verification would not provide the needed information, the plan is noted as unverified and returned for further revisions. If the needed verification is present, the plan is then accepted. The accepted plan may then be sent from the deception planning cell for integration with other C3CM and G2 plans.

Deception planning integrates the two main halves of the procedure, and also adds two new features. First, it shows the various kinds of knowledge and data required to perform each step of the process, and secondly, it shows the integration of the deception plan with other aspects of the C3CM plan and intelligence or G2 plans of the echelon involved. When the integration is complete, this new set of plans, monitored and controlled by the operations staff, is put into effect.

5. APPLICATION OF FRAMEWORK AND PLANNING PROCESS: REINFORCEMENT

The broadest application of deception would be to induce the OPFOR to take a course of action (COA) that would be optimal for the FFOR intentions. Such an application is likely to be feasible in practice only at a very high (e.g. operational or strategic) level for two reasons. First, it requires a large amount of resources and a long period of time to carry out a plan that leads the OPFOR into a course of action that it was not already planning. Second, as noted in FM 90-2, once such a plan is successfully carried out, it would be extremely difficult to initiate another similar plan in the future. These constraints are less critical at higher levels, particularly strategic ones, where events unfold over long time periods, where maximal resources are available, and where a single success can direct the entire future course of the conflict.

A narrower, but more practical application of deception is to seek and capitalize on instances where the OPFOR can be encouraged or reinforced to continue a course of action already initiated or planned (as against convincing him to take an entirely new tack). There are several kinds of benefits that can be achieved from this style of deception. First, if the OPFOR can be reinforced into a given COA, then the FFOR can be better prepared for OPFOR capabilities. In other words, it is easier to deal with an enemy if one knows what he is going to do. Second, the OPFOR could be reinforced into one specific COA (out of several possibilities) that gives a greater comparative battlefield advantage to the FFOR, given the FFOR's actual intentions and plans. The FFOR may have the best chance of succeeding in its plans if the OPFOR takes "option b", and so reinforcing the OPFOR to take option b by deception can increase the FFOR's battlefield advantage. (It should be noted here that comparative advantage may still be far from optimal; there might be yet another option, say option "d", that would give the FFOR the optimal advantage, but which was never considered as a viable option by the OPFOR commander. Thus, the OPFOR could not be guided into taking option "d" without recourse to a deception at the more global level that was rejected above.) And third, the reinforcement of an already-planned action is likely to be achievable with much fewer resources and on a repeatable basis. As noted in "Magruder's principle" in FM 90-2, the greatest "bang for the deception buck" is obtained when the object of the deception is led into doing what it planned to do or was prepared to do anyway.

There are two general stages in planning deception in this fashion. The first stage is understanding the tactical interactions and option spaces of the FFOR and OPFOR well enough to recognize situations in which OPFOR reinforcement leads to FFOR comparative advantage. The second step is understanding how and when OPFOR vulnerabilities to deception can be exploited to reinforce the desired OPFOR behavior. The overall concept of this reinforcement based deception is that of "going with the flow." The deception planner must first understand the likely flow of interaction between the FFOR and OPFOR so that points in the flow can be identified where a reinforceable OPFOR action will give the FFOR an advantage. Beyond that, the deception planner needs to understand both OPFOR vulnerabilities and FFOR deception resources well enough that a plan for exploitation of the opportunity for comparative advantage can be developed and implemented. While this knowledge about OPFOR vulnerabilities and FFOR capabilities can be very general, it can be usefully applied only after the deception planner's analysis of the battle flow has pointed out an OPFOR course of action that the FFOR would benefit by reinforcing.

Operationalizing the Reinforcement and Exploitation Process

Within this approach to deception planning, the critical requirement is to operationalize the more abstract conceptual results of the research in a way that allows a concrete planning aid to be built. The operationalization process breaks down into two tiers or levels, or corresponding to the two stages of deception planning just described.

Battle Flow Analysis — What to Reinforce

The first or upper-tier analysis that must be supported is an analysis of the battle process to identify the appropriate OPFOR actions or tendencies to reinforce. Such an analysis of the battle flow requires some model of the battle process. While it might seem at first that a full-blown digital battle simulator is necessary to carry out the analysis, this is really not the case. The deception planner does not need to be concerned with the physical details of the ongoing battle process (i.e., with specifics such as unit locations, casualties/attrition, logistics timetables, etc.). The concern is only with the higher-level logical ebb and flow of events — who moves to attack, who defends in place, who counterattacks, etc. It is extremely important to note that in typical operations, the range of options available in any given battle situation is highly constrained by the battle doctrine of each force. That is, given a specific battlefield situation, each commander will have a set of standard doctrinal tactics for dealing with that kind of situation. This is not to say that commanders never take bold or imaginative action; but it is to say that actions that are counter to doctrine are much rarer than those that conform to it.

The goal of this "battle flow" analysis is only to identify the space of likely options the OPFOR decision maker will perceive at any time, and to determine which (if any) of them might give the

FFOR a relative advantage given the FFOR's "true" goals. Given the assumptions listed above -- that a logical or abstract analysis will suffice, and that the space of options is strongly constrained by situation and doctrine — then the goal of the battle analysis can be met with a relatively simplified model. Such a model can be developed along the lines of a "wargame" or game theory model, in which the relationships between the two forces are organized into a move/countermove representation. The moves, in this representation, are the basic battlefield activities or tactics that define the logical level of interaction between the two forces. The effects of doctrine can be readily built into this structure as constraints on the range of actions or tactics that are available at any given time.

Such a representation is pictured in Figure 14. At some initial time, the FFOR has battlefield intention A and the OPFOR has a range of options based on how it perceives the FFOR's likely action. These options are depicted as B1, B2, and B3. Of these, the OPFOR commander decides on option B1, and associated actions b1. The FFOR commander, meanwhile, invokes action a, which is consistent with tactic A. This leads to some specific battlefield encounter between the FFOR and OPFOR, with some general results (e.g., FFOR intention A is partially met, and OPFOR intention B1 is largely met). This creates a new battlefield situation, in which the FFOR commander establishes a new action based on:

- the previous action,
- the battlefield situation (i.e., the result of the last actions), and
- the perception of the OPFOR's intentions.

The OPFOR commander makes a similar decision. In Figure 14, this leads the FFOR to consider only options C1, C2, and C3, and the OPFOR commander to consider options D1, D2, and D3. Each will select a specific intention from among these options, and put it into effect via a set of battlefield actions of the forces.

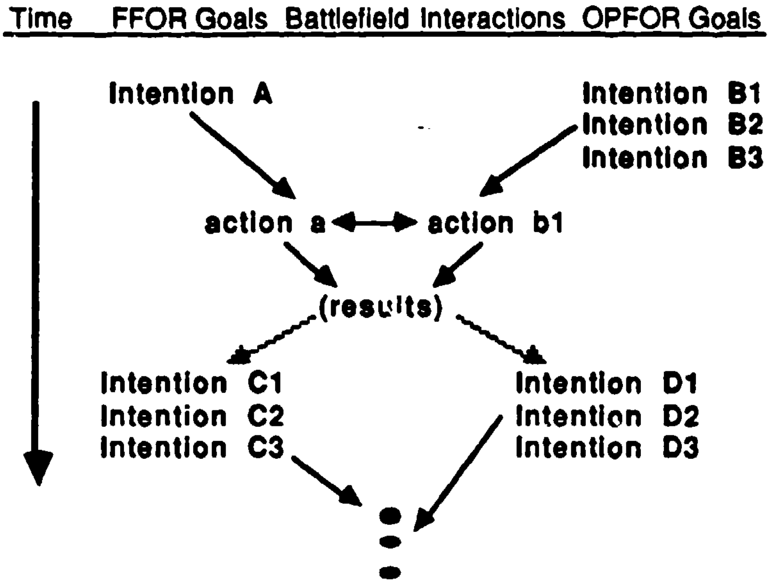


Figure 14. Conceptual act/react structure of battle flow

This pattern of interaction continues throughout the flow of the battle, and gives the flow an act-react structure.

This act-react representation of the battle process can be effectively modeled and the model used to help the deception planner identify OPFOR intentions to deceptively reinforce. The model is built by defining the general space of alternatives that are available on the battlefield — the 'universe' of reasonable tactics or intentions — and encoding how these alternatives are related to specific situations. This encoding can be done in various ways, but its goal is to capture the constraints on FFOR/OPFOR options that are encoded in each force's doctrine. Once developed, this model can be used to engage in a "what if" wargame style of analysis to determine how the OPFOR might react to a range of FFOR intentions, and to define a space of OFOR options at the current point in the battle. Then, this space can be analyzed to determine which might give the FFOR some relative advantage, and if so, how much advantage. This trade-off can then be used to select an OPFOR option that the FFOR should attempt to reinforce through deception.

Exploiting Vulnerability — How to Reinforce

Once this cognitive wargame analysis is used to define an OPFOR action to reinforce, the second tier of the deception planning process becomes involved. This tier of the planning process focuses on the "how" aspect, *i.e.*, how the FFOR should use its resources to deceive the

OPFOR into persisting with the action selected for reinforcement. It is the 'how' analysis that develops the actual content of the FFOR deception plan. The ultimate result of this second tier of analysis is the definition of specific actions that FFOR should take in order to provide the desired reinforcement. Using the terminology of Section 2, this is tantamount to exploiting an OPFOR vulnerability to deception. Thus, it first requires the deception planner to determine if the targeted decision is vulnerable.

Vulnerability is defined as the extent to which a given decision can be influenced by sensed data from the external world, specifically data that the OPFOR senses about the FFOR. A complete vulnerability analysis would required a detailed analysis or database about all OPFOR decision making procedures, indicating which data were used (and in which time frames) in making each OPFOR decision.

A simplifying assumption was made that all OPFOR decisions were assumed to be vulnerable to deception, but with the specific vulnerabilities defined by channels of information about the FFOR that could reach the OPFOR decision maker in the time frame of the decision. For example, suppose that the targeted decision X was made by the OPFOR division commander 18 hours before the actual action was to be taken. Thus, if a certain HUMINT channel that observed data on FFOR troop positions existed and if there further was a reporting chain that could bring these HUMINT data to the Division Commander no later than 18 hours before the time of the action, then it is assumed that this HUMINT data is capable of influencing that decision. Put differently, it is assumed that the decision X is inherently vulnerable to this HUMINT data.

This assumption allowed the vulnerability and exploitability analyses that comprise the second tier of the planning process to be adequately operationalized for inclusion in a planning aid. First, the specific decision maker who is responsible for any given decision targeted for reinforcement must be identified. This can be done with specific models of the OPFOR command and control structure, building on the general force descriptions given in previous documentation (Moan et al., 1989). Next, the vulnerabilities of this decision to deception are identified by mapping out the information channels that reach this targeted decision maker in the time frame in which the decision is made. While this is also a difficult process, it is far more constrained and feasible than mapping out the criteria for every OPFOR decision. Specifically, this analysis requires a database or model of the various sensing activities, nodes, and links that make up the OPFOR command and control or troop control system. These data are available, in the open literature, from various sources including C3CM studies and defectors. An analytical procedure must then be done to trace out the paths between the information sources and the targeted decision maker; this procedure has been termed *pathfinding*.

After it is completed, this pathfinding process identifies all the information sources that can reach the targeted decision maker within the time window of the decision. These therefore represent the space of OPFOR vulnerabilities to deception for the decision targeted for reinforcement. The next question, and the one that really addresses the content of the deception plan, is the question of how to exploit these vulnerabilities. This is where the two tiers of the analysis tie together. The upper tier or battle flow analysis identified two results — (1) an OPFOR decision that is targeted for reinforcement because it gives a comparative advantage to the FFOR's underlying operations plan, and (2) a FFOR intention or set of intentions that will reinforce the OPFOR's decision to undertake that targeted action. In other words, the through the battle flow analysis, the deception planner decides what action of the OPFOR he wants to reinforce, and then what FFOR action(s) will most likely induce that OPFOR COA response. This latter item can be combined with the list of OPFOR vulnerabilities to create a deception exploitation plan.

The OPFOR vulnerabilities define the filter through which the OPFOR views the FFOR actions. If the OPFOR determines that the FFOR is taking course of action Y, and consequently decides to take action X, the OPFOR will have done so only through those information channels that reach the decision maker who authorized action X. Conversely, if the FFOR wants to deceive the OPFOR into believing that its true intention is Y, then it must paint a picture using those channels on which the OPFOR is vulnerable. This is how the two levels of analysis are combined. The upper tier defines the FFOR action the FFOR wishes to portray (deceptively) to the OPFOR. The lower tier defines the channels on which the targeted OPFOR decision is vulnerable. Thus, the FFOR deception planner must determine how the FFOR intention to be portrayed will appear to the OPFOR on those vulnerable channels. To do this, the planner needs one more set of information, a set of data on how each FFOR action appears to the OPFOR. With this data, a final deception plan can be developed.

The next section discusses in more detail the formal ways in which these kinds of planning support are represented for incorporation into a computer-based deception planning aid.

6. SUPPORTING THE APPLICATION: DEFINING WITH TOOLS AND AIDS

The application of th^ search and analysis results to battlefield deception planning was then undertaken on two inte''r'lated tracks. The first track was development of a set of computer-based tools that would provide decision support to the two tiers of analysis defined in Section 6. These computer aids would provide focused support for certain key decisions in the deception planning process. On the broader level, though, the greater need for support for deception planning was seen to be a clear, well-structured process for developing deception plans. Accordingly, the second track of application was the development of a detailed "how-to" guide, along with supporting forms that could be used in a training or operational deception planning context. The steps and methods defined and documented in this second track were coordinated with the computer-based tools developed in the first track. That is, the overall deception planning process model not only provided a general procedure into which the individual computer aids would be used, but also provided specific guidance as to where and how these aids could and should be used in that process.

Computer Aids for Deception Pl^nning

Computer-based support was defined for the three specific functions arising from the analyses of Section 6.

- cognitive wargaming analysis of the FFOR/OPFOR act/react cycles
- pathfinding, and
- exploiting OPFOR vulnerabilities.

Each of these areas is discussed below.

Cognitive Wargaming

The conceptual act-react representation for the cognitive wargaming that could underlie deception planning had to be more rigorously defined before an actual tool to support it could be built. It is assumed that the continuous stream of action that characterizes a tactical engagement may be represented by a discrete sequence of moves and countermoves, as in the conceptual representation introduced in Section 5. Under this assumption, an appropriate model was developed, and is summarized below.

A tactical decision A is defined by a set of action options (or intention options) that are available to the decision maker. Thus,

A={a_i| a_i is an action option of decision A} , for the FFOR

There is also an associated set of OPFOR options:

A' ={a'_i| a'_i is an action option of decision A'}, A' is the OPFOR's decision corresponding to FFOR decision A

The idea of corresponding decisions refers to the fact that forces must interact in a tactical situation. Thus if a_i is a FFOR offensive move, then a'_i might be a doctrinally based responding defensive, evasive, or counteroffensive move. Note that for every FFOR tactical decision A (and OPFOR response/action A'), there will be some tactical result, or outcome. By defining the universe of possible FFOR actions as:

FF = {f_i| f_i is an action that the FFOR can take in some situation}, and

by defining the OPFOR action similarly as:

OF = {o_i| o_i is an action that the OPFOR can take in some situation},

the interaction of any two decisions is limited to the elements of FF x OF, subject to the given battlefield situation which can be denoted S. Battlefield outcomes can then be defined as a matrix, abbreviated OC(f,o|S). Each element in this matrix is interpreted as the outcome in terms of degree of satisfaction of FFOR goals, of FFOR action f and OPFOR action o in situation S. There is a corresponding matrix OC'(f,o|S), which refers to the outcome of FFOR action f and OPFOR action o in situation S, in terms of OPFOR goal o. As noted in Section 5., while a detailed simulation could be used to assess the values of OC, in general a much simpler categorization will be adequate for the deception planner's needs, such as "completely met goal, largely met goal, partially met goal, somewhat met goal, and completely failed goal."

While the outcome matrix relates OPFOR and FFOR intentions in a single move or cycle of the battle, another structure is needed to link the FFOR and OPFOR intentions across moves. This structure would represent the effect of doctrinal constraints on the range of decision options. This constraint can be defined by the relation Opt(o), which maps from a perceived OPFOR intention o to a subset of the space of FFOR intentions, i.e., onto the set FF. This relation specifies the range of FFOR actions or intentions that should be considered when the OPFOR is perceived to have intention o, according to FFOR doctrine. There is a similar relation Opt'(f) which maps from a perceived FFOR intention f to a subset of the space of OPFOR intentions, i.e., onto the set OF. This relation specifies the range of OPFOR actions or intentions that should be considered when the FFOR is perceived to have intention f, according to OPFOR doctrine.

Tactical decision-making (given this simple model), becomes the art of choosing that action f which maximizes the friendly force's outcome, i.e., which maximizes OC(f,o|S). Defined in this way, the decision problem is simple -- choose the alternative which yields the highest value in OC. Unfortunately, the optimal FFOR choice can only be determined by knowing what the opposing force's move will (or may) be doing. (The only time this isn't true is when the FFOR has one choice that is the best regardless of what the OPFOR does, an unlikely event). Thus, in most cases a decision strategy for choosing an optimal f will necessarily require an estimation of the OPFOR commander's decision o. If intelligence could predict with 100% certainty that OPFOR will make move o and no other, then FFOR's strategy would know with certain the optimal f. The decision strategy would be simple: select the row (f) from OC which, in column o, has the highest value. At best, this leaves the FFOR decision maker in a reactive mode, tailoring his action to an expected OPFOR intention.

This is where the concepts of deception planning and reinforcement come into play. The FFOR commander may, through the use of deception, influence the specific option the OPFOR commander chooses. In terms of the model, by portraying a deceptive image of the FFOR actions, the FFOR can influence the Opt' function by changing the OPFOR's estimate of the FFOR's intention (f) and thereby change OC. With appropriate models of Opt, Opt', OC, and OC', the deception planner can apply this logic in a variety of ways. For example, given a true intention of f, the deception planner can identify which OPFOR intention, say o*, maximizes the OC of f. Then, using Opt', it can be determind if that OPFOR intention o* is part of the Opt' for the current FFOR situation. If it is, then the deception planner can develop a plan to present to the OPFOR a picture of the FFOR intention that continues this appearance, so that OPFOR will be reinforced in a course of action which dictates that o* be selected.

This cognitive wargame analysis can be used to define a specific OPFOR intention to reinforce via deception, but many steps remain before this analysis is translated into a viable deception plan. One key step is identifying the OPFOR decision maker that is responsible for authorizing the targeted OPFOR intention. While the identification of the action could be made from an abstract model built around FFOR and OPFOR doctrine, this step requires a much more concrete model of how the FFOR and OPFOR command and control hierarchies function. Such a model could be developed directly from the analysis of FFOR and OPFOR decision cycles.

Pathfinding Analysis

Once the deception planner has identified an appropriate OPFOR action to reinforce and the OPFOR decision maker responsible for ordering/controlling that action, another set of key decisions comes into play. As discussed in Section 5, these decisions involve finding channels for feeding deceptive information to this targeted decision maker. In the terms of the underlying organizational model, this step involves identifying the targeted decision maker's vulnerability to deception. A second opportunity for computer aid was identified as supporting this pathfinding process.

The formal basis for the pathfinding tool is a command and control network model. This is a mathematical model that is organized according to the structure of the organizational information processing model developed at the start of the project (Figure 7, above). That model defined five stages of information processing in a C2 organization: sensing, analysis/interpretation, decision, planning/supervision, and action. That conceptual representation can be further refined by noting that these stages or processes correspond to both organizational and/or physical nodes in a given C2 system. Of the five stages of processing, decision making is best defined at the logical level. That is, a given physical node (e.g., a specific tactical operation center) may perform several functions of analysis/interpretation as well as decision and planning/supervision functions.

In the pathfinding process supported by network analysis tool, the specific concern is with the left side of Figure 7. This is the side which contains the paths that lead from sensing information about the FFOR to a given OPFOR decision node. Because the pathfinding tool was to be implemented as a computer-based aid, its structure had to be defined in formal terms. A mathematical command and control network model that corresponds to the logical model structure in Figure 7 was defined as follows:

let $N_o = \{n_o: n_o = \text{a sensing node}\}$

$N_i=\{n_i: n_i = \text{an intermediate/analysis node}\}$

$N_d=\{n_d:n_d = \text{a decision node}\}$

(For completeness, add

$N_p=\{n_p:n_p = \text{a planning/supervision node}\}$

N_a={n_a:n_a = an action node}

but note that N_p and N_a are ignored in the Pathfinding Tool). Information on the elements of N_o, N_i, N_d can be collected and maintained in an on-line database that could be searched either by the end-user directly or by the pathfinding tool in the course of its calculations.

The interconnections between the nodes — the links — are the key to the path analysis process. Links are mathematically represented as ordered pairs of nodes, e.g., as (n_i,n_j) with the order representing the flow of information. The pathfinding tool is concerned only with the *flow* or reporting of sensing information about FFOR behavior to higher OPFOR decision nodes. Thus, the notation (n_x,n_y) may be read as "node x reports to node y". The network is generally viewed as not symmetrical; thus (n_x,n_y) neither implies or precludes (n_y,n_x), at least in general. There are, however, restrictions on the links. Sensing nodes are assumed to report only to intermediate/analysis nodes, as indicated in Figure 7. Thus there are no links between members of N_o (i.e., (N_o,N_o) is an empty set). Intermediate analysis nodes may report to other intermediate nodes or to decision nodes, but not to sensing nodes. Decision nodes may report to other decision nodes, but not to intermediate nodes, and reporting within decision nodes is necessarily asymmetrical. (This corresponds to the notion of chain of command. A node will report to a superior node but not to a subordinate node; the information flowing in the opposite direction is command and control information, not sensing information.) The specific links that exist in any command and control network can also be specified in an on-line database, along with the information on the various nodes. The composite database that was constructed to support pathfinding and contained information on the node and link structure of the OPFOR, was denoted the OPFOR node/link database.

Specifying a pathfinding tool required its functionality to be defined. The pathfinding tool was defined to provide, as a comprehensive set, four functions for its user. The first is a automated analysis of a set of paths in a command and control network to identify the set of sensing nodes that feed information into a targeted decision node. Thus, the input to this process is a decision node n_d, and the output is a subset of N_o that contains the set of sensing nodes (and associated information paths) whose information ultimately reaches the targeted decision node n_d .

In practice, it is possible that this global path-collection function could be useless by itself, since it is likely to identify a large number of sensing nodes for any decision node. A typical Soviet Army commander ultimately receives information from virtually every sensing node in his Army. The function can made more useful by adding one or more constraining parameters to the path analysis process. Example parameters that could be added included:

- Time (T) — the time frame within which information has to travel from the sensing nodes to the decision nodes;
- Starting Time (S) — the specific point in time from which the information flow is to be analyzed; (S is meaningful only if T is also specified)
- Geographical Location or Range (R) — a geographical area to which the search for feeding source nodes is to be restricted. Source nodes outside R are excluded;
- Information Type or Form (F) — the kind of information to be considered, such as ELINT, HUMINT, etc..

This function, with parameters values specified, would allow the user of this tool to define a target node n_d, time frame for the deception, a geographical range for the deception, and the type of information that can be manipulated. In response, the planner will receive from the tool the set of sensing nodes, n_o, that are within the specific geographical locales and that will provide the specified kind of information on FFOR behavior to n_d within the time frame indicated.

This first pathfinding function provides a straightforward method for identification of the sensing nodes and paths through which targeted OPFOR decision maker is vulnerable. In some cases, such as where little time is available and/or an acceptable solution cannot provided by the constrained or unconstrained path collection function, other approaches may be needed. The planner may need to iterate the analysis by adjusting the parameter values to yield a larger or smaller set of source nodes to be targeted. Alternatively, the planner may need to take a more detailed look at the paths themselves and develop an alternate solution. This would require two additional tool functions.

These two additional functions are similar to each other, in that each focuses on the links associated with a single node in the network. The first of these is called the decision node analysis, and allows the deception planner to specify a given decision node, for which the tool will identify and display the set of intermediate nodes that provide information to that decision node. This allows the user to start path analysis by working backward from the targeted OPFOR decision maker. The other function is called the node star function, and is intended to work together with the first. The decision information node analysis allows the deception planner to start a computer-aided path analysis by identifying the elements of N_i that feed a given n_d; the node star analysis function allows the deception planner to trace these information feeder nodes back to sensing nodes in a flexible manner. Basically, this function allows the deception planner to define a given intermediate node, for which the tool will identify all intermediate decision, and sensing nodes that are connected to it. As with the decision information function, an information form parameter can be used to restrict the star to those links that report a certain kind of information. In addition, the user may also restrict the star to geographical regions, so that only parts of the star that are within a certain region of interest may be identified.

The node star analysis is intended to be used recursively in tandem with the decision information function, as follows. A targeted decision node is identified and its information feeders are defined via the decision information function. Next, the star of each of these feeders is examined via the node star analysis. The deception planner may note some commonality among their stars; the stars of these nodes are then examined themselves, leading to identification of sensing nodes that feed both/all of them. These sensing nodes may then be considered as the potential input location of deceptive information for the targeted decision node.

Used together in this way, the decision information and node star functions can yield the same result as the automated path analysis. By giving the deception planner direct control of the process by which the path(s) are generated and examined, it allows more solutions to be examined. In particular, it is expected that this cor.^uter-aided path analysis will be most important in cases where the automated analysis can not be done or yields an unacceptable solution.

The final function provided by a complete pathfinding tool is an ability to retrieve information on sensing nodes identified by either automated or computer-aided path analysis. This allows the deception planner to specify one or more sensing nodes, and retrieve any an all information in the node/link database on the sensing capabilities of those nodes. The purpose of this function is simply to allow the deception planner to evaluate his/her ability to provide information into any specific sensing node identified by the path analysis process as a potential source of deception information to the targeted decision maker.

In a complete 'mplementation, the pathfinding tool would be implemented as a detailed node/link database plus a set of algorithms that perform each of the four functions defined above:

- constrained and unconstrained automatic path identification,
- decision node analysis,
- intermediate node star analysis, and
- sensing node channel listing.

As discussed below in Section 7, the node/link database was implemented and used as the basis for the pathfinding portion of the automated deception planning tool. However, only the first and fourth functions were implemented in this tool, and they were implemented via precalculated or 'canned' solutions generated by off-line analysis of the node-link database. The second and third functions proved to be beyond the scope of the present effort, but remain as important candidate extensions of the current effort.

Exploiting OPFOR Vulnerability

The third major planning function that requires computational support involves deciding how to exploit the OPFOR vulnerabilities identified through pathfinding analysis. As discussed in Section 5, successfully exploiting OPFOR deception vulnerabilities required building a linkage between the pathfinding analysis and the cognitive wargaming analysis.

Using the notation for the battle flow given in earlier in this section,the options available to the OPFOR decision maker, given a perceived intention of the FFOR as f_i, are denoted Opt'(f_i). The value of Opt'(f_i) is in fact a subset of OF, the space of all possible OPFOR intentions. At this point in the planning process (i.e., after pathfinding, the deception planner will have an OPFOR intention oj which is targeted for reinforcement. Thus, to reinforce this intention, the planner needs to calculate the set F*, which is the set of all f_j such that o_j is an element of Opt'(f_j). This set F* identifies all FFOR intentions which, if perceived by the OPFOR, would lead the OPFOR to include the targeted action as part of its set of possible decision options. In general, the deception plan will be based on portraying to the OPFOR that the FFOR's intention is one of the elements of F*, or possibly even several intentions within F* in an ambiguous manner.

From this set F*, the deception planner then needs to determine how each intention, if carried out as an action, would appear to the OPFOR. There is a very large number of dimensions on which the observable signature of a given action could be defined. However, for purposes of deception, the only dimensions of interest are those channels included in the OPFOR vulnerable sensor suite identified by the pathfinding analysis. This set of sensors can be denoted N_O^*, a subset of the set N_O of all sensing nodes. If the channels or capabilities of any sensor n_O in No is defined as Chn(n_O), then the set CHN(N_O^*) of all channels by which a given FFOR action leading to the targeted OPFOR decision oj could be viewed is given by:

$$\mathrm{Chn}(n_o^*) = \bigcup_{n_o \Sigma N_o^*} \mathrm{CHN}(N_o^*)$$

The deception planner needs to define how each potential FFOR intention on F* appears to the OPFOR on each channel in CHN(N_O^*). From this, he can determine how much effort would be required to portray that intention to the OPFOR. This can involve many levels of tradeoff among resources available for deception, time available, and difficulty of the requirement. For example, of two choices in F*, one (call it f_i) may be 'visible' to the OPFOR in only two channels (e.g., certain kinds of electromagnetic emissions and certain troop movements) while the other (call it f_k) may be visible to the OPFOR on six or more channels. On the other hand, the second intention (f_k) may be more consistent with the FFOR past actions in the battle and may be much more likely to lead to the desired response from the OPFOR then the first one (f_i). In addition, there may be overlaps between two or more elements in F*. Continuing with the same example, two of the six channels on which the OPFOR can see action f_k may be the two on which the OPFOR can view f_i, and the appearance on these two channels may be the same for both FFOR intentions. Thus, a portrayal of the two dimensions f_i and one of the other dimensions of f_k would be completely consistent (from the OPFOR's viewpoint) with f_i and partially consistent with f_k. If the OPFOR's response to both were action o_m, then this would probably dually reinforce the taking of action o_m.

A tool to support this exploitation function would then have to provide computation of the following:

- calculation of F*, either automatically or in a machine-aided manner;
- identification of CHN(N_o*) from the pathfinding analysis results; and
- definition of the observable view of each f in F*, given the CHN(N_o*).

Planning Guidance and Training Workbook

The development of computer-based planning tools provides a clear, concrete means of support for key aspects of the deception planning process. The deception planning aids defined above were derived from a theoretical analysis of deception and a model of the processes underlying FFOR and OPFOR command and control. These computerized aids are intended to be used in the context of a comprehensive deception planning process that is an operationalization of ideas from this theoretical analysis and model. It is therefore important to note that, without access to this larger viewpoint on the planning process, the specific analytical tools may well have little utility. One of the conclusions developed early was that Army doctrine described only the end products of each step in deception planning, but had no clearly defined procedure for planning and executing battlefield deception. Little concrete detail existed on how (or whether) a deception annex to an Operations Plan should be constructed, what it should contain, or on what analyses it should be based. Thus, it was concluded that neither trainees nor operational personnel would generally share the global view of the deception planning process from which the tools were developed. For that reason, another set of products for the deception planner was designed, to define the specific planning process in which the formal analytical tools would be used.

This second set of application products consists of a paper manual and guidebook intended to specify the detailed process by which deception planning could be done. The planning process applies concepts from the theoretical results above and the general procedure outlined in Section 5 for implementing a reinforcement-based deception plan. It is intended to go beyond the current doctrinal levels and provide the deception planner with an enhanced deception planning process complete with analyses and tools to support that process.

7. IMPLEMENTATION AND EVALUATION OF DECEPTION PLANNING TOOLS AND AIDS

The planning aids and tcols described in the preceding section were implemented for subsequent evaluation and use in training and/or operational activities. The two planning aids are the Battlefield Activity Analysis Tool (BAAT) and the student/instructor guidebook. This section describes these aids, their implementation, and their evaluation.

In developing these materials, the focus could be placed either on the training phase or on the execution of deception planning in the field. Although the training focus was selected, application of these results could potentially affect all future deception planners. Also, the BAAT is designed to be relatively generic, considering abstracted rather than specific NATO and Warsaw Pact forces. It could not be applied pragmatically in any area without detailed (and Classified) additions or modifications to the data base, and would require such special tailoring in each operations area or theater. Training, on the other hand, deals effectively with abstracted (but realistic) scenarios, so the BAAT could be applied most conveniently and with few changes to a training context.

The Battlefield Activity Analysis Tool (BAAT) Implementation

The BAAT, a computer-based planning tool, was implemented in a stand-alone workstation/desktop computer. The actual computer environment for BAAT implementation was selected so as to make the tool maximally accessible to potential end users.

Hardware and Software Requirements

Most current desktop computing within the Armed Services is done on the IBM-PC compatible machines that were mass-purchased in or about 1986. The hardware configuration of this device defines the minimal requirements for BAAT, as follows:

- Zenith 248 model desktop computer, with IBM-AT compatible architecture, with
- 640Kb of RAM plus two 320Kb floppy disk drives,
- a 20Mb hard disk drive,
- monochrome monitor, and

- VGA graphics processor.

This minimal target class of computers is also highly available at other non-field locations within the Army (and also activities), thus making it a very flexible and general choice of hardware host. Within this hardware environment, the following software is the minimal requirement for BAAT:

- MS DOS operating system, release 3.2 or later,
- "dBASE III plus" ® database software.

The first is packaged with each Army Z248 machine, while the second is widely available throughout the Army.

Additional software tools were used to build the BAAT system. Microsoft C was used to program the bulk of the functionality of the BAAT code, because of the efficiency of the C language and its deep links with dBASE III plus and other software tools. The db_VISTA package was used to develop the portions of the BAAT that manage and process database queries. db_VISTA is a library of C routines that can search and retrieve information from dBASE III files with greater efficiency and flexibility than dBASE itself. db_VISTA produces standard C-language object code that can be distributed royalty free, and thus does not need to be purchased in order to run BAAT. Finally, the MetaWINDOWS graphics and windowing package was used to develop and support the user interface to BAAT, which can be based on both cursor and/or mouse tracking procedures, depending on the workstation configuration.

The dBase package is widely used and familiar to many people. Although it is sufficient for prototyping and creating small applications, it is not necessarily optional for large complex applications. C produces the highly optimized code desirable for a database application where there is frequent file retrieval and possible heavy computation, as expected in the Network Analysis tool. db_VISTA is a proven database management package written by a company (RAIMA) which has shown consistently that it will adequately support its product and its users.

BAAT Overview

The heart of the BAAT is a set of interconnected databases on generic FFOR and OPFOR courses of action (COA), action/reaction modelling data, and OPFOR sensor arrays. All data in the BAAT is Unclassified. These databases are logically organized into 3 separate but coordinated modules, as follows (see Figure 15):

- Intentions and observable actions COA databases, divided into

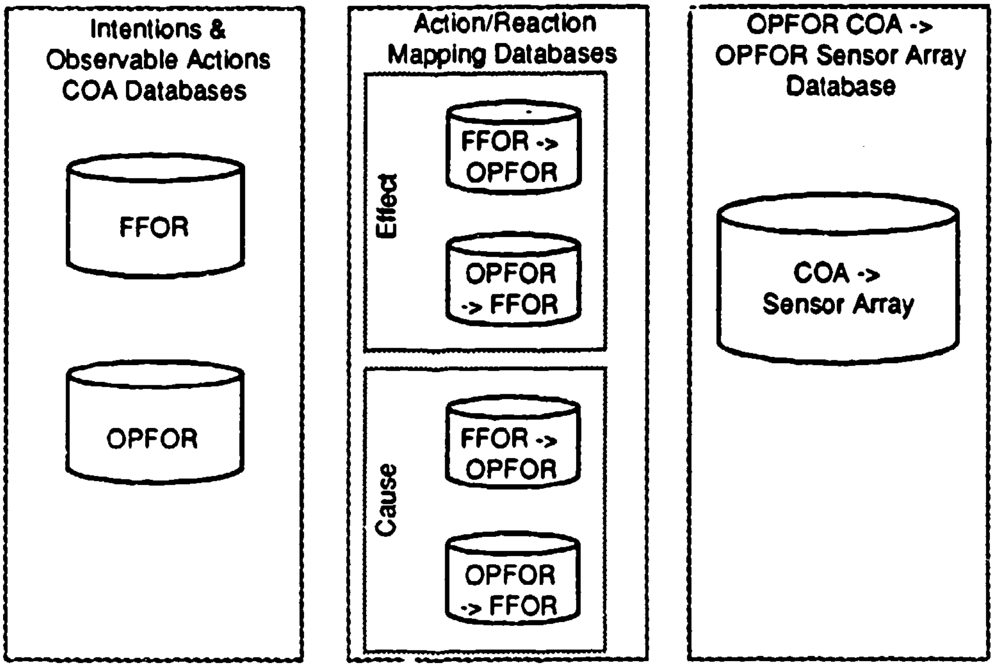


Figure 15. BAAT database organization

  - Friendly Force (FFOR) database, and
  - Opposing Force (OPFOR) database;
- Action/reaction mapping databases, divided into
  - FFOR action -> OPFOR reaction mapping database,
  - FFOR reaction -> OPFOR action causal mapping database,
  - OPFOR action -> FFOR reaction mapping database, and
  - OPFOR reaction -> FFOR action causal mapping database;
- OPFOR COA -> OPFOR sensor array database.

The COA databases contain related data on generic courses of action that can be taken by a given force. A course of action in this sense is defined to consist of a given intention (which may range from specific to very general) and a set of (observable) actions that the force takes in implementing the intention. In terms of the general action generation cycle discussed in Section 3 (cf. Figure 6), the intention is what is selected as the result of the Evaluate and Decide function, and observable actions are the results of the Act function that are "viewable" to the OPFOR. The two COA databases contain individual records, each of which is composed of an intention and a set of observable actions. Each record in these databases represents *most* of a COA. These relationships are illustrated below in equation form:

COA = intention + actions

I & O record = intention + observable actions

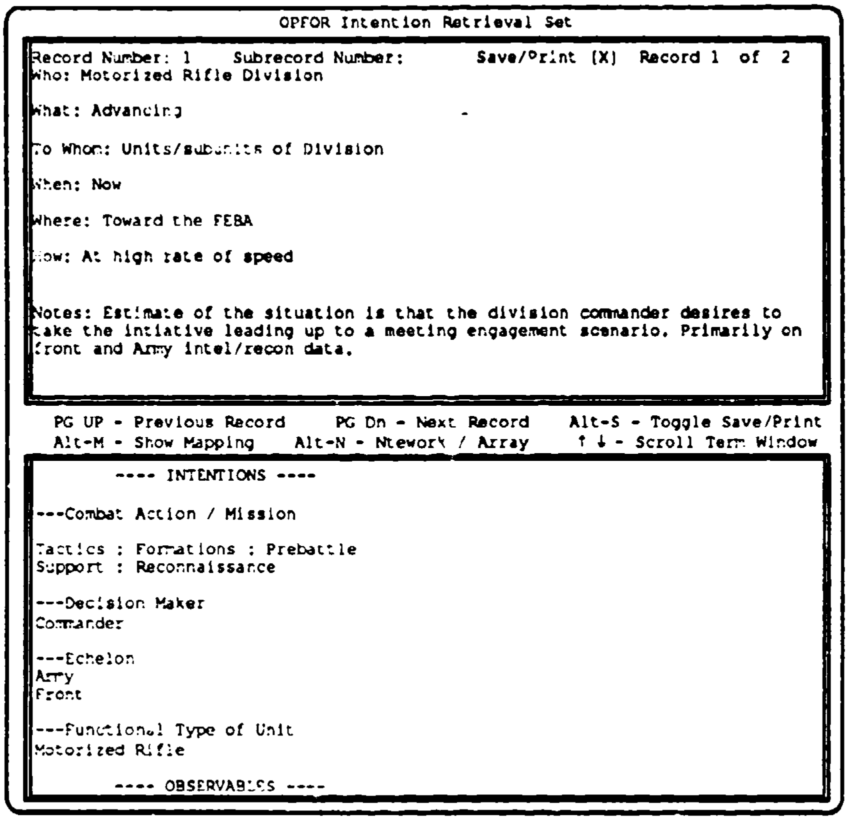
These two equations imply that:

I & O record = COA - unobservable actions.

Note that the "observable" actions may be *unobservable* to OPFOR for a variety of reasons. Some actions may be inherently unobservable to normal OPFOR intelligence or sensing mechanisms, e.g., FFOR commanders' decision processes. Others, however, may be observable in some circumstances and unobservable in others. For example, the OPFOR's normal ability to detect FFOR actions such as radio-electronic communications could be degraded by FFOR jamming actions, or simply by normal battlefield "fog and friction". The actions listed in the I & O records as "observable" are simply those actions which would *generally* be observable by the OPFOR. The handling of situation-specific cases left to the discretion of the deception planner (i.e., the BAAT user).

A sample OPFOR COA record, as it is displayed through BAAT, is shown in Figure 16. The intention is depicted at the top of display screen in a "Who, What, When, Where, Why" format, and the set of observable actions associated with that intention are shown at the bottom of the display screen. The separator between the intention and observable windows contains a number of switches and options, which are discussed in more detail in the BAAT Users Guide.

The FFOR COA database contains FFOR intentions linked to FFOR observable actions which experts say would be required/expected if FFOR were to carry out that intention, and that would generally be observable. The FFOR database currently contains 49 records, representing 49 generic US/NATO battlefield intentions. The OPFOR database contains OPFOR intentions linked to OPFOR observable actions which experts say would be required/expected if OPFOR were to carry out that intention, and that would generally be observable. The OPFOR database contains 65 records, representing 65 generic Soviet Army/Warsaw Pact intentions. These data are generic in that they are linked to no specific armies or theaters.

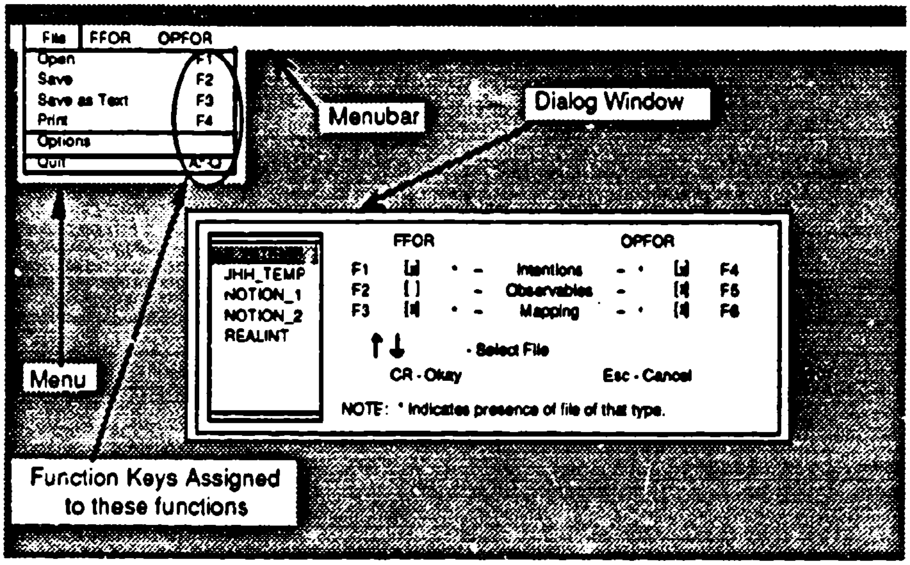


```
                        OPFOR Intention Retrieval Set
Record Number: 1    Subrecord Number:        Save/Print (X)  Record 1  of  2
Who: Motorized Rifle Division

What: Advancing

To Whom: Units/subunits of Division

When: Now

Where: Toward the FEBA

How: At high rate of speed


Notes: Estimate of the situation is that the division commander desires to
take the intiative leading up to a meeting engagement scenario. Primarily on
front and Army intel/recon data.


  PG UP - Previous Record     PG Dn - Next Record     Alt-S - Toggle Save/Print
  Alt-M - Show Mapping    Alt-N - Ntework / Array     ↑ ↓ - Scroll Term Window
          ---- INTENTIONS ----

---Combat Action / Mission

Tactics : Formations : Prebattle
Support : Reconnaissance

---Decision Maker
Commander

---Echelon
Army
Front

---Functional Type of Unit
Motorized Rifle

          ---- OBSERVABLES ----
```

Figure 16. BAAT COA database — sample OPFOR record

The action/reaction mapping databases contain links between FFOR intentions and OPFOR intentions. Thev are divided into cause and effect portions; each of these portions is further divided into OPFOR ==> FFOR and FFOR ==> OPFOR portions. Action/reaction mapping databases are hidden from the user of BAAT, in that they can not be explicitly searched as can COA databases. They are used by the BAAT only in conjunction with the "show mapping" option in the basic record display screen (see Figure 16). When the BAAT user selects this option, and a directionality, i.e. the causes (or antecedents) of the displayed intention versus the effects (or consequences) of the displayed action, the BAAT uses the appropriate mapping database to identify the corresponding FFOR or OPFOR intentions. These mappings are based on expert opinion of US Army and Soviet Army doctrinal responses to battle situations.

The BAAT provides the user with a flexible interface for searching the COA databases. The BAAT user can search by any aspect of an intention, such as the types of units involved, the class of intention involved, or the class of observable activity associated. Figure 17 shows an example of the capabilities and organization for the BAAT database search interface.



NOTE: * Indicates presence of file of that type.

Figure 17. Search Interface

The action/reaction mapping databases allow the BAAT user to identify the various act-react options between the FFOR/OPFOR pair. They specifically allow the deception planner to see how the OPFOR commander's options change as an understanding of the current FFOR intentions changes. Put differently, it allows the deception planner to view what responses the OPFOR might make under different deceptive portrayals of FFOR intentions. This analysis forms the basis for identifying what specific deception options are available. This use of the BAAT accomplishes the first of the three planning support functions defined in section 6 above, the cognitive war-gaming analysis of act/react cycles.

The second deception planning function identified in Section 6 was pathfinding. This function concerns identifying the OPFOR decision maker that is the desired target of a deception plan, and determining the channels by which deceptive information can be provided. Earlier, a large database (the C2 node-link database) representing the structure of both the US/NATO (FFOR) and the Soviet Army/Warsaw Pact (OPFOR) was built. This database identified various command and control nodes in each organizational structure, and various communication links that connected these nodes. The purpose of the C2 node-link database was to allow very complex and sophisticated tracing and analysis of the possible communication paths from OPFOR sensors to targeted OPFOR decision makers.

In integrating this node-link database with the COA databases it was determined that there was inadequate memory and computational power within the Zenith Z248-class computer. Although several alternatives were explored, an analytical solution to this problem was developed and is described below.

Each record in the COA databases defines a possible tactical intention of a given force, along with the observable actions associated with it and the conditions under which it is usually indicated. In reviewing this record structure, it became clear that the specific decision maker responsible for each operational activity to be undertaken was well-defined, and could be stored as part of the record in the database. This suggested an alternative way of integrating the node-link database (and the path-finding task it supports) with the COA databases (with the deception target development task it supports). The targeted decision maker and the information paths could be analyzed separately (using the node-link database) for each record in the COA databases. This would define the decision maker who could authorize each activity along with the sensors that provide the information on FFOR activity to this decision maker. Then, the path-finding results could be entered into the COA database record and permanently stored (as an essentially "compiled" path finding analysis).

Performing these path finding analyses revealed that, although the OPFOR C2 structure is complex, there are only a few decision makers who can authorize the actions stored in the OPFOR COA database. Thus, even though the path-finding problem is conceptually complex, the nature of military command showed that it was in practice very constrained. The small number of empirical path-finding solutions were calculated using the C2 node-link database and stored directly in the appropriate records in the OPFOR COA database.

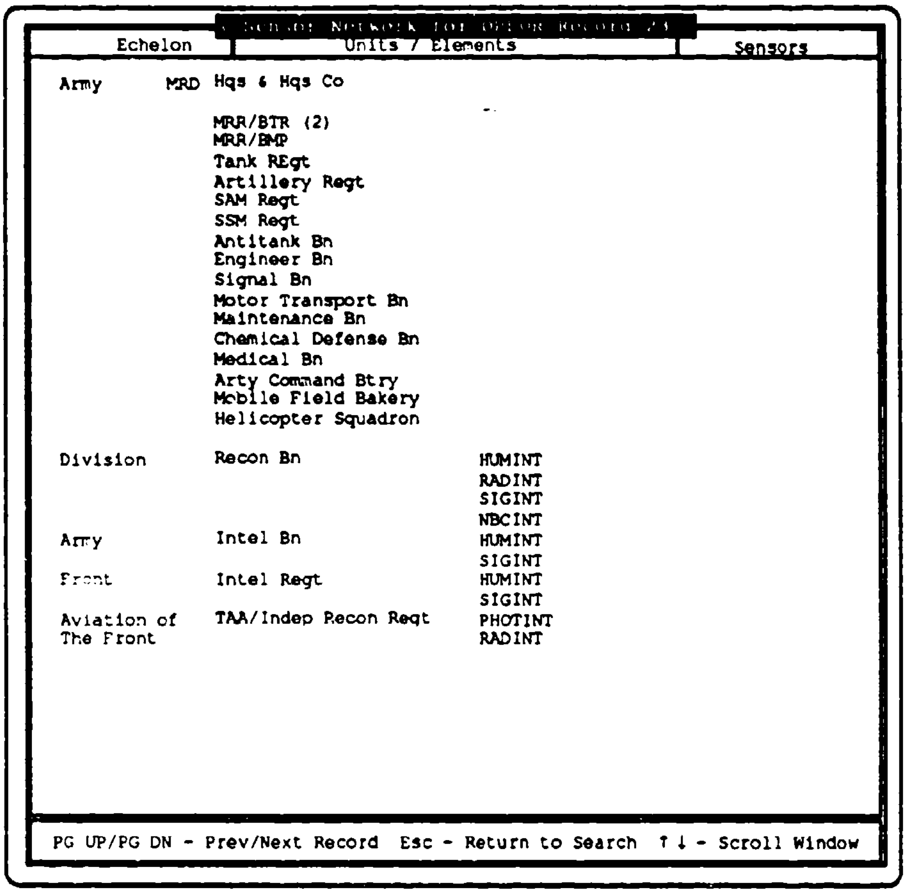
In practice, this offers another benefit. Rather than maintaining the strict analytical separation between the path-finding and target development steps, this solution acted to increase their conceptual integration to the BAAT user. Once the user found an OPFOR activity amenable to deception, the decision maker that would be the target of the deception process (and his information sources) is directly displayed on the screen as part of the record. The basic BAAT display of a COA database record also shows an example of the display of the responsible OPFOR decision maker and the OPFOR sensors and information sources that provide information to this decision maker in the context of this decision. This can be seen on Figure 16, above.

A related goal of the path finding analysis is to identify the specific sensors through which the OPFOR would be vulnerable to deception on a given COA. This information was also integrated into the BAAT through the OPFOR COA -> OPFOR sensor array database. The OPFOR COA -> OPFOR sensor array database is hidden from the BAAT user similar to the action/reaction databases. It is accessed by the BAAT software in conjunction with requests to view the array of OPFOR sensors that are used in conjunction with a particular OPFOR COA. This is done by selecting the Network/Array option from a BAAT display of an OPFOR COA record. An example of this array is shown in Figure 18. It is based on expert opinion of likely Soviet decision maker priorities among available intelligence collection means, in the situation specified by the currently selected record. This information is based on analysis of the paths through which critical information might percolate up to the decision maker, and on knowledge of Soviet Army intelligence collection, decision cycles, and troop-control doctrine.

An additional function of the planning tool was to help identify the observable FFOR behavior that would lead the OPFOR to believe the desired notional FFOR intention. This helps the planner in determining what a given FFOR intention would "look like" to the OPFOR, given the OPFOR's sensing capabilities. Understanding the signature of a FFOR intention, in turn, assists the deception planner in constructing a deception plan that will appear realistic and consistent to the OPFOR. This data is incorporated into the basic record structure of the COA databases. Once a given OPFOR COA is selected, the BAAT user can automatically view the observable (to the OPFOR) actions associated with it, as shown in Figure 16 above. It is notable that this BAAT function requires the same BAAT databases (COA and mapping) as does the first function. Thus, no additional elaboration of the basic database structure was required to incorporate support for this function into BAAT.

Guidebook for Deception Planning

The second major planning aid from this effort is a guidebook, consisting of a set of manuals and materials intended to support the deception planning process and the training of deception planners. While the BAAT provides automated support and data for the deception planning process, it is important that the BAAT be accompanied by a guide to the deception planning process as well as a step-by-step manual for actually conducting deception planning.



```
                 Sensor Network for OPFOR Record 23
       Echelon     |          Units / Elements          |     Sensors

Army        MRD Hqs & Hqs Co

                MRR/BTR (2)
                MRR/BMP
                Tank REgt
                Artillery Regt
                SAM Regt
                SSM Regt
                Antitank Bn
                Engineer Bn
                Signal Bn
                Motor Transport Bn
                Maintenance Bn
                Chemical Defense Bn
                Medical Bn
                Arty Command Btry
                Mobile Field Bakery
                Helicopter Squadron

Division        Recon Bn                HUMINT
                                        RADINT
                                        SIGINT
                                        NBCINT
Army            Intel Bn                HUMINT
                                        SIGINT
Front           Intel Regt              HUMINT
                                        SIGINT
Aviation of     TAA/Indep Recon Regt    PHOTINT
The Front                               RADINT

PG UP/PG DN - Prev/Next Record  Esc - Return to Search  ↑↓ - Scroll Window
```

Figure 18. BAAT OPFOR sensor array database — sample record

As a result, a set of integrating materials adaptable for teaching and practicing deception planning were developed. These materials were incorporated into a guidebook for deception planning consisting of a student workbook and an instructor's annex. These materials considered the entire planning process, and also include detailed guidance on how the BAAT tool should be used at various steps in the process. The underlying logical flow of the deception process, as developed in the Workbook and Instructor's annex, is shown in Figure 19. There, the process is divided into six sequential steps, with key decision criteria for continuation to be applied after each step. Figure 19 essentially maps the sequence of steps involved in deception (as discussed in Section 3 and Figure 9) onto a set of concrete actions that occur or are observed from within the FFOR deception planning cell.

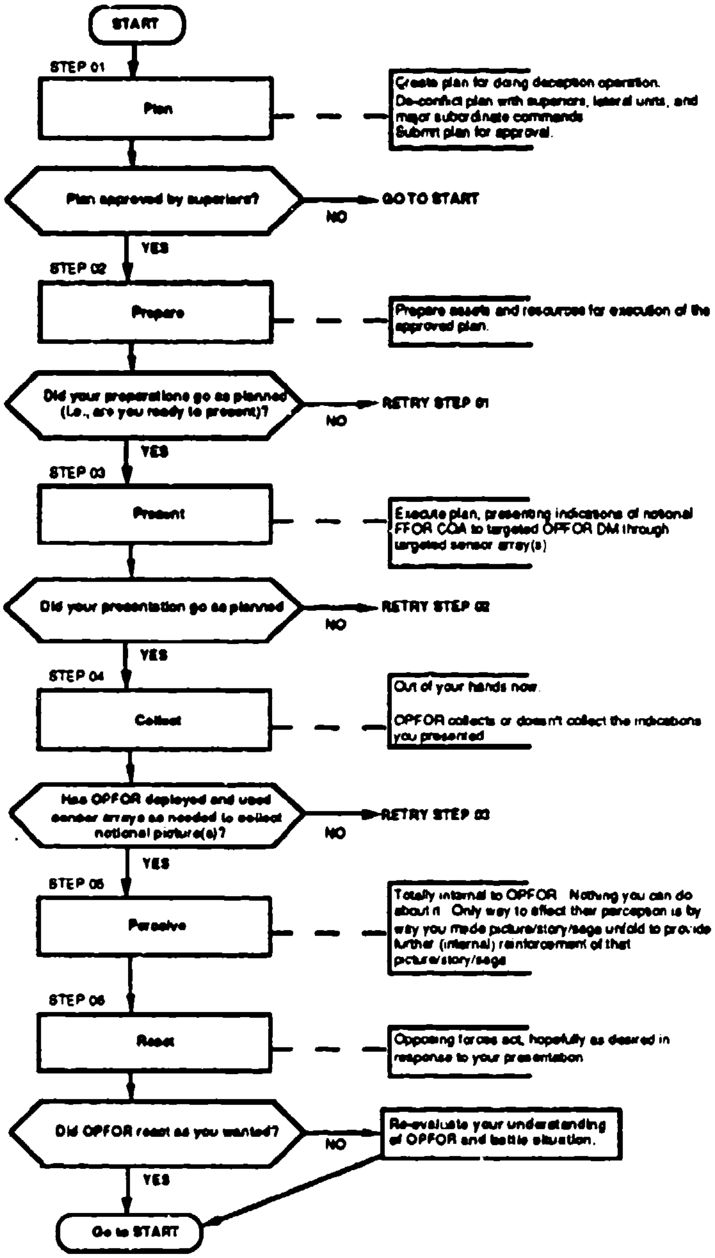

START
STEP 01
Plan
Create plan for doing deception operation.
De-conflict plan with superiors, lateral units, and major subordinate commands
Submit plan for approval.
Plan approved by superiors?
NO
GO TO START
YES
STEP 02
Prepare
Prepare assets and resources for execution of the approved plan.
Did your preparations go as planned (i.e., are you ready to present)?
NO
RETRY STEP 01
YES
STEP 03
Present
Execute plan, presenting indications of notional FFOR COA to targeted OPFOR DM through targeted sensor array(s)
Did your presentation go as planned
NO
RETRY STEP 02
YES
STEP 04
Collect
Out of your hands now.
OPFOR collects or doesn't collect the indications you presented
Has OPFOR deployed and used sensor arrays as needed to collect notional picture(s)?
NO
RETRY STEP 03
YES
STEP 05
Perceive
Totally internal to OPFOR. Nothing you can do about it. Only way to effect their perception is by way you made picture/story/saga unfold to provide further (internal) reinforcement of that picture/story/saga
STEP 06
React
Opposing forces act, hopefully as desired in response to your presentation
Did OPFOR react as you wanted?
NO
Re-evaluate your understanding of OPFOR and battle situation.
YES
Go to START

Figure 19. Deception process flow chart

More detailed guidance is also provided in the Student Workbook and Instructor's Annex for the planning steps (i.e., steps 1, 2, and 3 in Figure 19). This planning guidance is summarized in the chart in Figure 20 which depicts the logical flow of deception planning. The workbook discusses in detail how the various features of BAAT are used to support the analysis required at each step in Figure 20. It also provides a series of templates, forms, and notations for carrying the development of a deception plan through from start to finish. Finally, several example problems

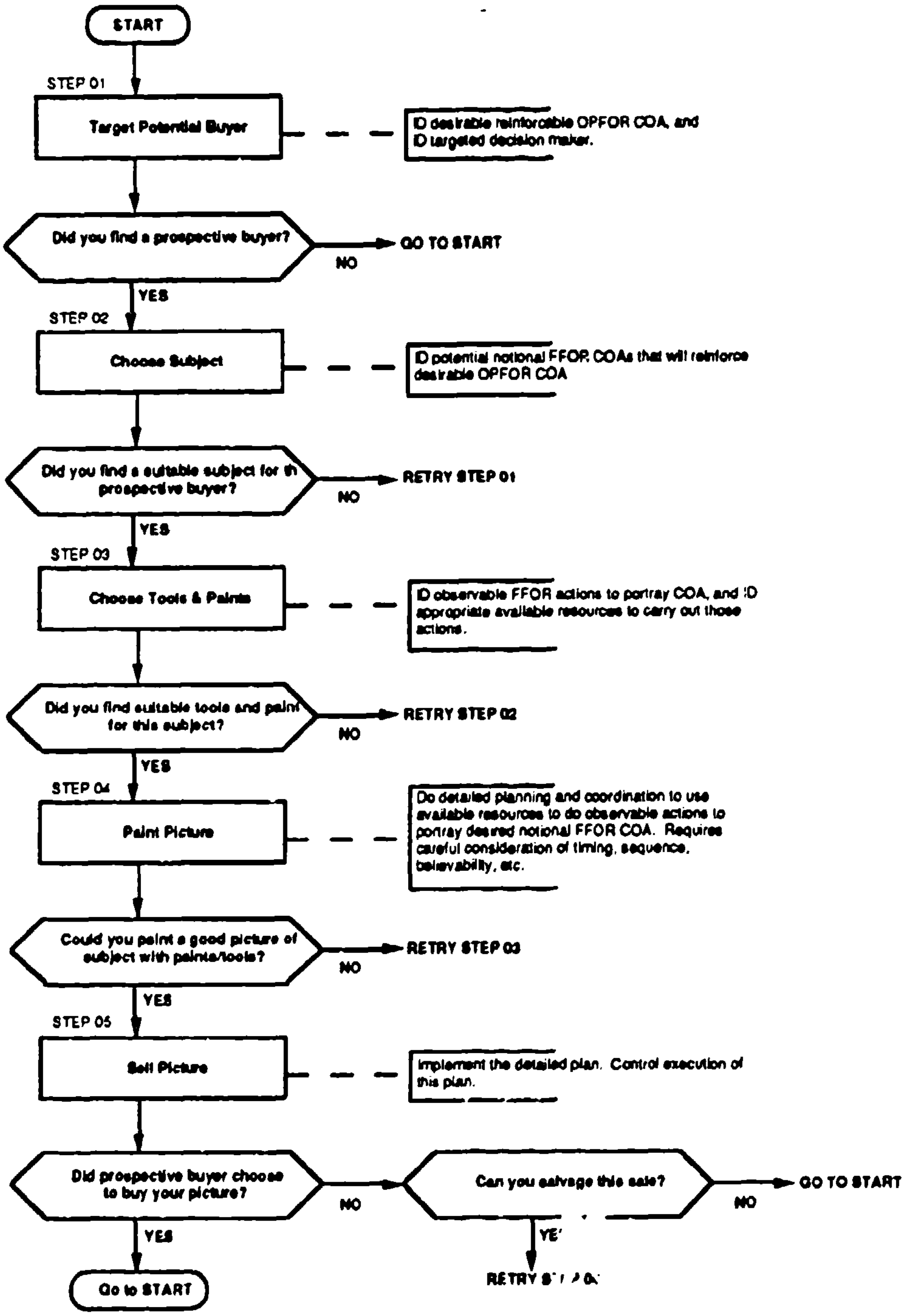

START
STEP 01
Target Potential Buyer
ID desirable reinforcable OPFOR COA, and ID targeted decision maker.
Did you find a prospective buyer?
NO
GO TO START
YES
STEP 02
Choose Subject
ID potential notional FFOR COAs that will reinforce desirable OPFOR COA
Did you find a suitable subject for th prospective buyer?
NO
RETRY STEP 01
YES
STEP 03
Choose Tools & Paints
ID observable FFOR actions to portray COA, and ID appropriate available resources to carry out those actions.
Did you find suitable tools and paint for this subject?
NO
RETRY STEP 02
YES
STEP 04
Paint Picture
Do detailed planning and coordination to use available resources to do observable actions to portray desired notional FFOR COA. Requires careful consideration of timing, sequence, believability, etc.
Could you paint a good picture of subject with paints/tools?
NO
RETRY STEP 03
YES
STEP 05
Sell Picture
Implement the detailed plan. Control execution of this plan.
Did prospective buyer choose to buy your picture?
NO
Can you salvage this sale?
NO
GO TO START
YE'
RETRY S' ' ⁄ 0
YES
Go to START

Figure 20. Deception planning steps flow chart

are included. One example is included in the Student Workbook, and three aspects of this problem are discussed in detail. Two other example problems (without solutions) are also included in the Instructor's manual. All examples are based on the TRADOC Common Teaching Scenario.

Evaluation of Deception Planning Aids

In order to accomplish an evaluation of the utility of the deception planning aids described above, it would be necessary to construct an evaluation research design to compare aided and unaided deception planning performance. This design would need to include:

- selection of appropriate setting,
- construction of problem scenarios,
- specification of measures of effectiveness (MOEs) for rating the differential performances of the aided and unaided conditions,
- selection of appropriately selected and trained planners as subjects, and
- design of data collection and analysis procedures.

Since deception planning is the activity of interest, the most natural MOE for this situation would be some measure of the "goodness" of a deception plan. For example, how likely is the developed plan to deceive the OPFOR in this situation (and in general)? How consistent and verifiable is the plan? How efficient is the plan in its use of FFOR resources? Essentially what is required is a valid cost-benefit assessment methodology for a deception plan.

An alternate approach for deception plan MOEs is to look at the battle outcome, or the effect of a given deception plan on the eventual outcome of the engagement. This approach is in principle more satisfactory, because the engagement outcome MOE is obviously of central importance to the commander. However, such an approach also presents severe obstacles, as it requires an analytical means to relate specific deception plan alternatives to battle outcomes, or a deception-sensitive engagement model. These MOE difficulties are not unresolvable, since research is being conducted in these areas, particularly in the development of large-scale engagement models.

8. SUMMARY AND CONCLUSIONS

This effort has been directed toward increasing the understanding of the nature of battlefield deception. The results of this effort span a very wide range of potential application to Army (and other service) field operations. These include the following areas:

- *doctrine* — the Army currently has little in the way of formal deception doctrine. FM 90-2 was in preparation during most of this research, and even in its complete form deals with only some aspects of the problem. Results such as the deception taxonomy and organizational information processing model could be used to generate doctrinal material that would supplement the conceptual approach of FM 90-2 (and other service manuals).

- *planning tools and aids* — the Army has few standard tools or aids for the deception planning process. Those specific operational units that practice deception in their operations have developed local techniques and aids, but these have not been formally evaluated or disseminated. The models and concepts developed in this research could thus be used to develop decision aids, database, or other planning tools and aids that could support the deception planning process on an Army-wide basis.

- *procedures and operational concepts* — similar to the situation with tools and aids, the Army has virtually no standard procedures for deception planning. While there is a organizational entity in G3 that is called the deception cell, operational concepts are in development to guide its activities and their integration with the larger operations planning and intelligence analysis processes. The models and concepts developed in this project could also be applied to developing detailed procedures for deception call actions, and operational concepts for integrating deception cell activities into the larger activities of Corps and Division G3 and G2.

- *materiel development* — the Army (and other service elements) has a substantial array of deception materiel, from inflatable tanks to EW decoys and emulators. However, most of this materiel development has been technology driven, with little a prior concern for the tactical impact or use of the materiel items. The deception taxonomy in particular could be used to organize the existing materiel according to the means and ends its serves, and to further guide the deception materiel development process to emphasize those deception activities that currently have little or no materiel support.

- *tactical development* — similar to the situation with planning procedures and planning aids, there has been little development of battlefield tactics for deception or of the relevance of various tactics to deception. The global framework provided by the taxonomy and FFOR/OPFOR models could be used to guide such analyses, which could then be used to supplement deception doctrine and procedures.

- *training and training aids* — an active program of deception training has been implemented to train deception cell members and to parallel the development of deception doctrine (via FM 90-2). However, for various reasons this training is only loosely coupled with the procedures and operational practice of deception. The overall deception framework developed in this research could be used to create instructional materials, training approaches, and even training aids for the deception school.

In evaluating these various options, it was decided that the most desirable avenue for applying and following-up on the research results described above was to seek near-term fieldable applications . An emphasis on near-term application was seen to have several benefits. It would:

- provide an immediate and greatly needed support to the Army in actual deception operations,
- serve to assess the relevance of the research findings to operational needs,
- help identify deficiencies and weaknesses in the research framework,
- allow early research results to be tested via operational use, and
- clarify the needs of the operational community for further research and analysis.

The focus on near-term applications, however, also created several constraints. Application in operational use or operational training settings, for example, meant that any application products had to be made consistent with Army styles and formats, as well as with Army procedures and doctrine. This, in turn, meant that the relevant issues in the application setting had to be identified and learned as part of the application process.

A further review suggested that the greatest short term impact would be the development of specific aids and tools to support both the near-term *training* of deception planners and the eventual *operational practice* of deception.

Results have been achieved in three areas: theoretical and conceptual models, deception-related methods, and tangible products. There is a logical flow of these results, from models to methods to aids. This flow has focused on understanding and manipulating the OPFOR military perceptions and actions, thus complementing current US Army doctrine on deception.

With respect to theoretical and conceptual models, a "psychological framework" was defined as a two-part construct, consisting of:

1. A taxonomy of concepts and components of deception, providing a hierarchical *language* with which to talk about deception.
2. A highly general tactical decision making model to represent the concept of decision cycle as an *organizational* phenomenon.

This framework provided a theoretical context for the development of deception planning methods and aids.

Using this general framework, several methods were developed to examine deception in a more specific context, that of the US/NATO vs. Soviet/Warsaw Pact forces:

1. Cognitive-science analysis and enhancement of current doctrinal deception planning process.
2. A simplified conception of battlefield engagement as an *act-react* cycle, containing the concepts of *reinforcement*, *intentions* and *observables*, and *pathfinding*.

These methods provided specification of data and knowledge needed to effectively conduct battlefield deception.

Based on identified knowledge needs, planning aids and tools were designed, consisting of two parts:

1. A PC-based decision aid, called the *battlefield activity analysis tool (BAAT)*. The BAAT assists the planner in answering the key questions needed to conduct battlefield deception.
2. A deception planning *guidebook* accompanying the BAAT, which consists of a student workbook and an *instructor's annex*. The guidebook both explains the logical flow of deception and works through tactical examples using the BAAT.

Suggested Future Research and Development

This effort has focused on conceptual models dealing with the cognitive or human-thought aspects in the decision-making process. Emphasis was given to analytical tools and aids which can assist the deception planner and the ultimate decision maker in their respective roles. In particular, this approach has focused on "knowing the enemy" as the crucial prerequisite to deceiving him. Understanding Soviet Army decision making processes at division, army, and front levels is the only way to fully exploit his vulnerabilities to deception. To continue development of the models, methods, and tools begun here, an essential next step would be an all-source investigation that focuses on critical decision-making elements, particularly the commander's decision cycle and methodology, and the role of the staff control organs. Such an investigation would directly benefit the deception planner by providing insights to vulnerabilities in the OPFOR's decision-making system. Several specific areas within this investigation appear particularly fruitful:

- *Soviet Army tactical network planning and control (NPC) methodology.* Design and develop a model of a Soviet Army NPC to assist in more realistic simulations in war games. The work already done in this project on critical path analysis can serve as a basis for further research and development.

- *Soviet Army commander's intentions on the battlefield.* Design and develop, in close cooperation with intelligence, models to assist in more accurate assessments of OPFOR intentions.

- *Soviet Army radic electronic combat (REC) doctrine, systems, and operations.* Use all-source analysis in gaining a better understanding of REC and ways to exploit it on the battlefield employing deception and other C3CM capabilities.

- *Soviet Army sensor array analysis.* Conduct a vigorous all-source analysis effort of the OPFOR's primary sensor array supporting battlefield requirements from division to front levels.

- *Profiles of Soviet Army commanders and chiefs of staff.* Design and develop clone models of OPFOR key decision makers in order to aid deception planners and friendly commanders in targeting their specific weaknesses and vulnerabilities.

As the above studies are carried out, the increased knowledge would facilitate further development of the methods and tools described above, and provide impetus for new methods and tools. Some of these directions are:

- *C3I training employing deception tools/aids.* Design and develop simulator tools/aids for deception planning support in simulation and wargaming exercises involving the C3I decision-making system.

- *US Army intelligent deception planning tool.* Design a model/process for developing deception concepts and options in support of the commander's specific mission, tailored to set situations and circumstances.

- *Profiling.* Extend the models and techniques to include individual variations in and multi-layer cultural effects on OPFOR decision makers, based on the obtained OPFOR profile information.

- *Vulnerability analysis.* Develop, elaborate, and formalize the relationships between organizational characteristics and vulnerability to deception.

- *Act-react cycle development.* Extend and formalize the act-react cycle, including the process of behavioral extinction (as well as reinforcement).

- *Pathfinding.* Extend and develop the proposed capabilities for the pathfinding tool, as described in Section 6.

Implementing these extensions and new avenues of study can provide benefits for deception planning, training, and doctrine.

REFERENCES

Amarel, S. (1981). *Problems of representation in heuristic problem-solving: related issues in the development of expert systems.* (Tech. Rep. CMB-TR-118.) New Brunswick, NJ: Rutgers University Laboratory of Computer Science Research.

Amarel, S. (1982). *Expert behavior and problem representation.* (Tech. Rep. CBM-TR-126). New Brunswick, NJ: Rutgers University Laboratory of Computer Science Research.

Card, S., Moran, T. and Newell, A. (1983). *The psychology of human-computer interaction.* Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Cimbala, S.J. (Ed.) (1986). Soviet C3. *Signal,* Vol. 41, No. 4 (Special Issue).

Dempster, A.P. (1968). A Generalization of Bayesian Inference. *Journal of Royal Stat. Society,* 30, 205-247.

Druzhinin, V.V. and Kontorov, D.S. (1977). *Concept, algorithm, decision.* Soviet Military Thought Series. No. 18. Moscow. (Translation, HQ U.S. Air Force, Washington, DC).

Glantz, D.M. (1985). *The red mask: the nature and legacy of Soviet military deception in World War II.* Carlisle, PA: US Army War College, Center for Land Warfare.

Handel, M. (1982). Intelligence and deception. *Journal of Strategic Studies.* Vol. 5, pp. 112-154.

Hemsley, J. (1982). *Soviet troop control.* New York, NY: Brassey's Publishers.

Heuer, R.J., Jr. (1981). Cognitive factors in deception and counterdeception. In Daniel, D.C., and Herbig, K.L., *Strategic Military Deception.* New York: Pergamon Press.

Malone, T.W. (1989). Organizing information processing systems: Parallels between humar organizations and computer systems. In Robertson, S., Zachary, W., and Black, J. (Eds.) *Cognition, Computation, and Cooperation: a multidiscipline study of cooperative systems.* Hillsdale, NJ: ARLEX Press.

Moan, K.L., Broz, A.L., Zaklad, A.L., Bulger, J.P., Hicinbothom, J., and Knapp, B. (1990). *A comparative overview of OPFOR and FFOR decision cycles for battlefield deception planning* (ARI Research Report 1551). Alexandria, VA: US Army Research Institute. (AD A221 199)

Newell, A., Shaw, J. and Simon H. (1959). Report on a general problem-solving system. In *Proceedings of the International Conference on Information Processing* (UNESCO). Paris.

ORD (Office of Research and Development) (1978). Misperception literature survey. Washington, DC: Central Intelligence Agency.

ORD (Office of Research and Development) (1981). *Deception maxims: fact and folklore.* Washington, DC: Central Intelligence Agency.

ORD (Office of Research and Development) (1982). *Deception failures, non-failures, and why.* Washington, DC: Central Intelligence Agency.

Pylyshyn, Z. (1984). *Computation and cognition.* Cambridge, MA: The MIT Press.

Savelyev, V.P., Fhemanskiy, P.V. and Ivanov, D.A. (1977). *Fundamentals of tactical command and control.* Soviet Military Thought Series. No. 18. Moscow. (Translation, HQ U.S. Air Force, Washington, DC).

Schafer, G. (1976). *A Mathematical Theory of Evidence.* Princeton, NJ: Princeton University Press.

Simon, H.A. (1981). *Sciences of the artificial* (2nd edition). Cambridge. MA: MIT Press

U.S. Air Force. (1989). *Deception Planning Guide.* Joint Special Operations Deception Course.

US Army. (1982). *Operations.* Field Manual 100-5 Washington, DC: US Army Headquarters.

US Army. (1984a). *Staff Organization and Operations.* Field Manual 101-5. Washington, DC: US Army Headquarters.

US Army. (1984b). *The Soviet Army — Operations and tactics.* Field Manual 100-2-1. Washington, DC: US Army Headquarters.

US Army. (1984c). *The Soviet Army — Troops Organization and Equipment.* Field Manual 101-2-3. Washington, DC: US Army Headquarters.

US Army. (1985). TRADOC Common Sense Scenario. Washington, DC: US Army Headquarters.

US Army. (1987) . *Battlefield Deception* Field Manual 90-2 . US Army Intelligence Center and School.

Wohl, J.G. (1981). Force Management Requirements for Air Force Tactical Command and Control. In *IEEE Transactions on Systems, Man, and Cybernetics,* Vol. SMC-11, No. 9, pp. 618-639.

Zaklad, A., Zachary, W., Broz, A., Moan, K., Bittner, A., and Hicinbothom, J. (1988). *Development of a framework for battlefield deception: opposing force OPFOR decision structure analysis and disruption.* (TR 2074-1, Vol. 1) Willow Grove, PA: Analytics, Inc.

Zaklad, A., Zachary, W., Broz, A., Moan, K., Bittner, A., and Hicinbothom, J. (1988). *Development of a framework for battlefield deception: opposing force OPFOR decision structure analysis and disruption.* (TR 2074-1, Vol. 2) Willow Grove, PA: Analytics, Inc.

Zaklad, A., Zachary, W., Bittner, A., Broz, A., Hicinbothom, J., and Knapp, B. (1988). *Doing Deception: Attacking the Enemy's Decision Processes.* (TR 2074-3) Willow Grove, PA: Analytics, Inc.

Zaklad, A., Moan, K., Zachary, W., and Knapp, B. (1988). *A framework for tactical deception.* ARI Working Paper HUA 88-04. Alexandria, VA: US Army Research Institute.